

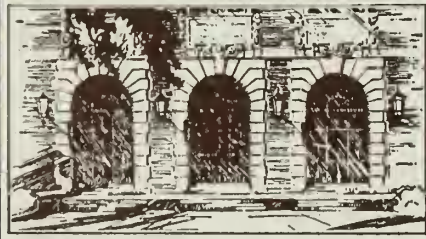
LIBRARY OF THE
UNIVERSITY OF ILLINOIS
AT URBANA-CHAMPAIGN

510.84

I l 6r

no.188-199

cop. **2**



510.84
IL6v
no. 192
pp. 3

ON THE STRUCTURE AND AUTOMORPHISMS OF FINITE AUTOMATA

by

Zamir Bavel

October 1, 1965

RECEIVED

JAN 27 1966

BRAN



DEPARTMENT OF COMPUTER SCIENCE · UNIVERSITY OF ILLINOIS · URBANA, ILLINOIS

The person charging this material is responsible for its return on or before the **Latest Date** stamped below.

Theft, mutilation, and underlining of books are reasons for disciplinary action and may result in dismissal from the University.

University of Illinois Library

OCT 22 1961

L161—O-1096

ON THE STRUCTURE AND AUTOMORPHISMS OF FINITE AUTOMATA*

by

Zamir Bavel

October 1, 1965

Department of Computer Science
University of Illinois
Urbana, Illinois

* This work was submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Mathematics, October, 1965.



Digitized by the Internet Archive
in 2013

<http://archive.org/details/onstructureautom192bave>

ACKNOWLEDGEMENT

The author wishes to express his deep gratitude and appreciation to Professor Franz E. Hohn for the guidance, encouragement, inspiration, professional and personal stimulation, helpful comments and advice, and the privilege of association he has given the author, and for the painstaking and conscientious critique he has given this thesis.

The author wishes to express special thanks to Professor David E. Muller for the many helpful conversations, out of which came the motivation for this thesis, for his willingness and readiness to help, and for his critical assistance and collaboration in the past two years.

The author also wishes to acknowledge and thank the Danforth Foundation for the two years of the Danforth Teacher Grant, without which this thesis and the work leading to it would have been impossible.

TABLE OF CONTENTS

	Page
0. INTRODUCTION	1
1. MINIMAL AUTOMATA	8
2. GENERATORS AND PRIMARIES	14
3. SOURCE	19
4. HOMOMORPHISMS AND SOURCE	31
5. MINIMAL AUTOMATA, CYCLES, AND AUTOMORPHISMS.	40
6. PRIMARIES AND AUTOMORPHISMS.	57
7. EXTENSIONS OF AUTOMORPHISMS.	62
8. ADDITIONAL RESULTS AND POSTSCRIPT.	80
BIBLIOGRAPHY	87
VITA	89

0. INTRODUCTION

In this section we establish the notational conventions and list the basic definitions in the theory of automata, which we use in the following sections. We also describe the content and explain the organization of the paper in brief.

The term "automaton" is to mean "finite automaton" throughout the paper. As we are not concerned with the output feature of sequential machines, we ignore both the set of outputs and the output function in the definition of an automaton.

0.1. Definition: An automaton A is a triple (Q, I, δ) , where Q is a finite set (the set of states), I is a non-empty semigroup (the input semigroup), and δ is a function (the transition function) on $Q \times I$ into Q , which satisfies $\delta(q, xy) = \delta[\delta(q, x), y]$, for all $q \in Q$ and for all $x, y \in I$.

This definition is similar to those of Fleck [5], Rabin and Scott [1], and Ginsburg [3], but with the set of outputs and the output function deleted from the latter. These three definitions differ from # 0.1 mainly in that we allow the set, Q , of states of the automaton A to be empty; i.e., $Q = \emptyset$.

0.2. Definition: The automaton $(\emptyset, I, \delta)$, whose set of states is the empty set $\emptyset$, is called the empty automaton and is denoted by $A(\emptyset)$.

Clearly, $A(\emptyset)$ depends neither on I nor on δ . Hence, except for notational differences, there is essentially a unique empty automaton.

For the sake of brevity, we sometimes omit the word "automaton". In such cases, the unreferenced letter A denotes an automaton $A = (Q, I, \delta)$. Similarly, the unreferenced letter Q denotes the set of states of A .

An alternative, but for our purposes equivalent, definition of an automaton is one which emphasizes the input alphabet, M , from which the input semigroup is generated.

0.3. Definition: An automaton A is a triple (Q, M, δ) , where Q is a finite set (the set of states), M is a non-empty finite set (the set of inputs, or the input alphabet), and δ is a function (the transition function) on $Q \times M$ into Q . Where M^* is the set of all finite sequences of elements of M (including the sequence of length zero, or the empty input, denoted by ϵ), δ is extended to $Q \times M^*$ by the rule: $\delta(q, xy) = \delta[\delta(q, x), y]$, for all $x, y \in M^*$, after the manner of [1] and [3].

Rabin and Scott [1] showed that the elements of M , together with the operation of concatenation (juxtaposition), generate a free semigroup X . We obtain the semigroup I (or more precisely, an isomorphic copy of I for a given automaton) by regarding two elements, x and y , of X as equivalent if, and only if, they define the same function on the set of states of the automaton; i.e., $x = y \iff \delta(q, x) = \delta(q, y)$ for all

$q \in Q$. We shall use definitions ## 0.2 and 0.3 interchangeably, with M denoting the set from which I is generated.

0.4. Definition: Let $A = (Q, I, \delta)$. We denote by I^* the augmented input semigroup of A , where the elements of I^* are the empty input, ϵ , and the elements of I , and where $x\epsilon = \epsilon x = x$, for all $x \in I^*$.

The natural generalization of an automaton appears in the following definition.

0.5. Definition: A monadic algebra A is a triple (Q, M, δ) , where Q is the set of elements of A , M is the set of operation indices of A , and δ is the transition function $\delta: Q \times M^* \rightarrow Q$ of A , with the property, $\delta(q, xy) = \delta[\delta(q, x), y]$ for all $q \in Q$ and for all $x, y \in M^*$.

Thus, an automaton is a finite monadic algebra; i.e., a monadic algebra with a finite set, Q , of elements (and hence a finite set, M , of non-redundant operation indices). The term "algebra" is to mean "monadic algebra" throughout this paper.

0.6. Definition: An automaton $A = (Q, I, \delta)$ is said to be strongly connected if, and only if, for any $p, q \in Q$, there exists $x \in I$, such that $\delta(p, x) = q$.

0.7. Definition: Let $A = (Q, I, \delta)$ and let $P \subseteq Q$. Then, $B = (P, I, \delta^0)$ is said to be a subautomaton of A , denoted $B \ll A$, if, and only if, for all $p \in P$ and for all $x \in I^*$, $\delta^0(p, x) \in P$, where δ^0 is the restriction of δ to $P \times I$.

The reader will note that, for any two subautomata, B and C , $B \ll C$ and $C \ll B \iff B = C$. For any $B \ll A$, we denote the set of states of B by Q_B , unless this set is explicitly given a different denotation. At times, when no ambiguity may arise, we use the same symbol, δ , for the transition functions of both an automaton and its subautomaton.

We make use of the customary notation of set theory and, where we apply it to automata, rather than to sets, we state the sense in which the symbols are used. Here, we need only point out that, where B is a subset of states of an automaton (Q, I, δ) ,
 $- B \stackrel{\text{def}}{=} Q - B$.

As a result of typographical restrictions, we use the symbol "#" in three different ways: Where B is a set, $\#(B)$ denotes the cardinality of B . We further use "#" to specify the numerical label of a result (e.g., # 3.2 refers to the label of the lemma which appears as the second labeled item of section # 3). Lastly, in lemma # 5.20 we define a group operation and denote it by "#". In each case, the context will make clear the sense in which this symbol is used.

We now detail the organization, and briefly describe a part of the content, of the remainder of the paper.

In section # 1, we define a minimal automaton and illustrate some of the advantages it affords.

In section # 2, we formulate the basic notion of a primary of an automaton and that of the generators of the primary. We show that the set of primaries of an automaton is both unique and exhaustive, but the fundamental nature of the primary is investigated more fully in succeeding sections.

In section # 3, we formulate the basic notion of the source of a subset of states and explore its use. We illustrate the characterization via the source of such notions as: strong connectedness, separated subsets of states, discrete automata, retrievable automata (see Bavel - Muller [10]), and reflexive automata. We also indicate further uses for the source.

In section # 4, we introduce homomorphisms, endomorphisms, isomorphisms, and automorphisms on automata and study their application to the notion of source. Some of the results we obtain thus are these: Any endomorphism on a strongly connected automaton is an automorphism. The source of a strongly connected subautomaton B is invariant under an automorphism which maps a state of B into B . Two homomorphisms, which have the same image on a state, q , are identical on the subautomaton generated

by q . The homomorphic image of a discrete algebra is discrete. The homomorphic image of a reflexive algebra is reflexive.

In section # 5, we introduce the notion of a cycle (a generalization of the classical cycle) and use it to characterize and count all automorphisms of a minimal automaton (m.a.). We show that any such automorphism is completely determined by its action on any generator of the m.a. and that any two such defining cycles (of the same automorphism) are either identical or disjoint. Furthermore, we show that the order of such an automorphism in the automorphism-group of the m.a. is equal to the length of the defining cycles and that this length divides the cardinality of the set of generators of the m.a. We show that the set of automorphic images of any state, q , of a m.a. A , with the analog " $\#$ " of functional composition as the operation, forms a group which is a homomorph of the automorphism-group, $G(A)$, of A and that, if q is a generator of A , the said group is an isomorph of $G(A)$. We show that the order of the automorphism-group of a m.a., A , divides the cardinality of the set of generators of A and, as a corollary, we obtain the following generalization of a theorem of Fleck [5]: The order of the automorphism-group of a strongly connected automaton, A , divides the number of states of A .

In section # 6, we apply the notions and results of previous sections to the primaries of an automaton. We show that every primary of the homomorphic image of an automaton is the

image of some primary of the automaton; that the automorphic image of a primary is a primary; that the set, $P(A)$ of automorphisms leaving all primaries invariant is a normal subgroup of the automorphism-group; that the order of any member of $P(A)$ is the l.c.m. of the lengths of the defining cycles in all the primaries of the automaton.

In section # 7, we study the nature, behavior, and number of the members of $P(A)$ via extensions of automorphisms of one primary to another. We introduce the notion of a component, study its behavior under automorphisms, and use it to reduce the scope of the investigation. We characterize and count all extensions of an automorphism of a primary, R , to a primary, S , and thus are able to characterize and count all members of $P(R \cup S)$. We also indicate the extension of this process to the entirety of $P(A)$.

In section # 8, further results by the author, based on this paper, are briefly described and some tempting directions of further investigation are indicated.

1. MINIMAL AUTOMATA

We shall need the following notational conventions for sets of successors and the few elementary results concerning them.

1.1. Definition: Let $A = (Q, I, \delta)$ be an automaton with $R \subseteq Q$. Then,

- (i) $\delta(R) = \{\delta(r, x) : r \in R, x \in I\};$
- (ii) $\delta_0(R) = \{\delta(r, x) : r \in R, x \in I^*\};$
- (iii) $\delta(r) = \delta(\{r\}), r \in Q;$
- (iv) $\delta_0(r) = \delta_0(\{r\}), r \in Q.$

We note that $\delta_0(R)$ contains the successor of each state in R by the empty input, ϵ , while $\delta(R)$ may not.

1.2. Lemma: Let $B, C \subseteq Q$, where $A = (Q, I, \delta)$. Then,

- (i) $\delta(B \cup C) = \delta(B) \cup \delta(C); \quad \delta_0(B \cup C) = \delta_0(B) \cup \delta_0(C).$
- (ii) $\delta(B \cap C) \subseteq \delta(B) \cap \delta(C); \quad \delta_0(B \cap C) \subseteq \delta_0(B) \cap \delta_0(C).$
- (iii) $B \subseteq C \implies \delta(B) \subseteq \delta(C) \quad \text{and} \quad \delta_0(B) \subseteq \delta_0(C).$
- (iv) $\delta_0[\delta(B)] = \delta[\delta_0(B)] = \delta(B); \quad \delta_0[\delta_0(B)] = \delta_0(B).$

Proof: (i) $q \in \delta(B \cup C) \iff$ there exists $p \in B \cup C$ and $x \in I$, such that $q = \delta(p, x) \iff$ there exists $p \in B$ such that $q = \delta(p, x)$ or there exists $p \in C$ such that $q = \delta(p, x)$, for some $x \in I \iff q \in \delta(B)$ or $q \in \delta(C) \iff q \in \delta(B) \cup \delta(C).$

(ii) $q \in \delta(B \cap C) \implies$ there exist $p \in B \cap C$ and $x \in I$, such that $q = \delta(p, x) \implies q \in \delta(B)$ and $q \in \delta(C) \implies q \in \delta(B) \cap \delta(C).$

(iii) Let $q \in \delta(B)$. Then, there exist $p \in B$ and $x \in I$, such that $q = \delta(p, x)$. But, $B \subseteq C \implies p \in C \implies q \in \delta(C)$.

The proofs for the second part of (i), (ii), and (iii) are identical to those for the corresponding first part, with δ_0 replacing δ and I^* replacing I .

(iv) This is immediate from the definition # 1.1.

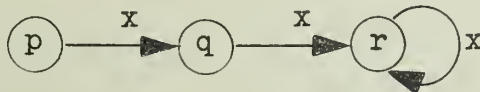
Q.E.D.

The following example demonstrates that the inclusion in # 1.2 (ii) cannot be replaced by equality: Let $Q = \{p, q, r\}$, $M = \{x\}$, and $\delta(p, x) = \delta(q, x) = \delta(r, x) = r$.



Here, $\delta(\{p\} \cap \{q\}) = \delta(\emptyset) = \emptyset$, while $\delta(p) \cap \delta(q) = \{r\}$.

The following example demonstrates that # 1.2 (iv) cannot be strengthened to read: $\delta[\delta_0(B)] = \delta_0(B)$ and $\delta[\delta(B)] = \delta(B)$. Let $Q = \{p, q, r\}$, $M = \{x\}$, $\delta(p, x) = q$, $\delta(q, x) = \delta(r, x) = r$.



Here, $\delta_0(Q) = Q$, $\delta[\delta_0(Q)] = \delta(Q) = \{q, r\} \neq \delta_0(Q)$, and $\delta[\delta(Q)] = \delta(\{q, r\}) = \{r\} \neq \delta(Q)$.

One of our main devices, which we define in # 1.3, below, is the minimal automaton containing a given subset, P , of

the set, Q , of states of an automaton; i.e., the automaton generated by P .

1.3. Definition: Let $P \subseteq Q$, where $A = (Q, I, \delta)$.

The minimal automaton of P , denoted by $A(P)$, is defined by,

$$A(P) = \cap \{B \ll A : P \subseteq Q_B\}.^{(1)}$$

When P is a singleton ($P = \{p\}$), we omit the set designation, so that $A(p) \stackrel{\text{def}}{=} A(\{p\})$, as there is no danger of ambiguity.

The reader will note that both the definition and the notation in # 1.3 are consistent with those of the empty automaton, $A(\emptyset)$, of definition # 0.2.

It is easily seen that the intersection of subautomata is itself a subautomaton, since the successors of each member of the intersection are members of each intersected subautomaton and, hence, are themselves members of the intersection. Thus, $A(P) \ll A$, for all $P \subseteq Q$.

1.4. Definition: Let $P \subseteq Q$, where $A = (Q, I, \delta)$.

The automaton generated by P , denoted by $[\delta_0(P)]$, is defined by,

$$[\delta_0(P)] = (\delta_0(P), I, \delta'),$$

where δ' is the restriction of δ to $\delta_0(P) \times I$.⁽²⁾ Again, we omit the set designation when P is a singleton, so that, if $P = \{p\}$, $[\delta_0(p)] \stackrel{\text{def}}{=} [\delta_0(\{p\})]$.

⁽¹⁾ The intersection of subautomata (P_i, I, δ_i) , $i \in \{1, 2, \dots, n\}$, is taken to be the triple, (P, I, δ') , with $P = \bigcap_{i=1}^n P_i$ and δ' is the (common) restriction of the δ_i 's to $P \times I$.

⁽²⁾ Y. Give'on formed a similar definition concurrently and independently in [9].

The reader will note that $[\delta_0(P)] \ll A$, since the closure of δ^0 is guaranteed by the definition. It is also clear that $P \subseteq Q[\delta_0(P)]$.

1.5. Theorem: For all $P \subseteq Q$, $A(P) = [\delta_0(P)]$.

Proof: The comment preceding the theorem implies that $A(P) \ll [\delta_0(P)]$, by ## 1.3 and 1.2 (iii). Conversely, $A(P) \ll A \implies \delta_0(P) \subseteq Q_{A(P)} \implies [\delta_0(P)] \ll A(P)$.

Q.E.D.

In view of # 1.5, we shall use definitions ## 1.3 and 1.4 interchangeably.

Some of the utility of the concept of minimal automata may be seen from the (trivial) fact that any subautomaton of A is the union of the minimal automata of its states. As we intend to use this fact implicitly, we shall dignify it by stating it as a theorem, but its proof is trivial and, hence, omitted.

1.6. Theorem: $B \ll A \implies B = \bigcup \{A(q) : q \in Q_B\}$. (3)

As we shall make use of the following two known results (for example, see [3], p. 30) concerning strongly connected automata, we take this opportunity to further illustrate the

(3)

The union of subautomata (P_i, I, δ_i) , $i \in \{1, 2, \dots, n\}$, is taken to be the triple (P, I, δ^0) , with $P = \bigcup_{i=1}^n P_i$ and δ^0 is the restriction of δ to $P \times I$.

utility of the minimal automaton, which we employ in our proofs of these results.

1.7. Theorem: Every automaton has a strongly connected subautomaton.

Proof: Any one-state automaton is clearly strongly connected. Suppose the theorem true for all k -state automata, where $k < n$, and let $A = (Q, I, \delta)$ be an n -state automaton with q as one of its states. If $A(q)$ is not strongly connected, then there exists $p \in \delta(q)$ such that, for all $x \in I^*$, $\delta(p, x) \neq q$. But, $A(p) \ll A(q)$ and $q \notin \delta_0(p) \implies \#[Q_{A(p)}] < \#[Q_{A(q)}]$. Hence, by the inductive hypothesis, $A(p)$ has a strongly connected subautomaton and, therefore, so does A . Thus, the theorem is proved by induction.

Q.E.D.

An automaton B is said to be a proper subautomaton of an automaton A if, and only if, $B \ll A$, $B \neq A$, and $B \neq A(\emptyset)$.

1.8. Theorem: An automaton is strongly connected if, and only if, it has no proper subautomaton.

Proof: Suppose $A = (Q, I, \delta)$ has no proper subautomaton. Then, for all $q \in Q$, $A = A(q)$ and, hence, for all $p, q \in Q$, there exists $x \in I^*$, such that $p = \delta(q, x)$. Thus, A is Strongly connected.

Conversely, if A is strongly connected and $A(\emptyset) \neq B =$

$(P, I, \delta) \ll A$, then, for all $q \in Q$ and for all $p \in P$, there exists $x \in I$, such that $\delta(p, x) = q$. Hence, $q \in \delta_0(p) \subseteq \delta_0(P) \Rightarrow Q \subseteq \delta_0(P) \Rightarrow A \ll B$. Thus, $A = B$.

Q.E.D.

2. GENERATORS AND PRIMARIES

We now make use of the concept of a minimal automaton to define a basic building block of automata, -- the primary. As will be seen later, the primaries of an automaton are of major importance, and may be frequently used to an advantage.

2.1. Definition: Let $B \ll A$. A subset $R \subseteq Q_B$ is said to be a generating set of B (alt., to generate B) if, and only if, $B = \bigcup_{q \in R} A(q)$. A state $q \in Q_B$ is said to be a generator of B if, and only if, $B = A(q)$. If $B = A(p)$, the set of generators of B , denoted by $\text{gen } B$, is defined by,

$$\text{gen } B = \{q \in Q_B : A(q) = B\}.$$

As shown in # 2.5 below, every automaton has a non-empty generating set. However, the set of generators is defined only for minimal automata.

2.2. Lemma: Let P be a generating set of $A = (Q, I, \delta)$. Then, for each $q \in Q$, there exists $p \in P$, such that $A(q) \ll A(p)$.

Proof: Let $P = \{p_1, p_2, \dots, p_n\}$, and let $q \in Q$. P generates $A \implies A = \bigcup_{i=1}^n A(p_i) \implies q \in \bigcup_{i=1}^n \delta_0(p_i) \implies q \in \delta_0(p_j)$, for some $j \in \{1, 2, \dots, n\} \implies \delta_0(q) \subseteq \delta_0[\delta_0(p_j)]$, by # 1.2 (iii). Hence, by # 1.2 (iv), $\delta_0(q) \subseteq \delta_0(p_j)$ and, thus, $A(q) \ll A(p_j)$.

Q.E.D.

It should be noted that p_j (in the proof of the lemma # 2.2) is not necessarily unique; i.e., there may exist $p_k \in P$, distinct from p_j , such that $A(q) \ll A(p_k)$.

We illustrate the use of a generating set by showing that the definition of an abelian automaton is equivalent to a weaker statement. An automaton $A = (Q, I, \delta)$ is said to be abelian (see, for example, [5]) if, and only if, for all $q \in Q$ and for all $x, y \in I$, $\delta(q, xy) = \delta(q, yx)$.

2.3. Theorem: An automaton is abelian if, and only if, for any generating set P of A , $\delta(p, xy) = \delta(p, yx)$, for all $p \in P$ and for all $x, y \in I$.

Proof: Let P be any generating set of $A = (Q, I, \delta)$, and let $q \in Q$. Then, by # 2.2, there exists $p \in P$, such that $q \in \delta_0(p) \implies$ there exists $z \in I^*$, such that $q = \delta(p, z) \implies$ for all $x, y \in I$, $\delta(q, xy) = \delta[\delta(p, z), xy] = \delta(p, zxy) = \delta[p, z(xy)] = \delta[p, (xy)z] = \delta[p, x(yz)] = \delta[p, (yz)x] = \delta[\delta(p, yz), x] = \delta[\delta(p, zy), x] = \delta[\delta(p, z), yx] = \delta(q, yx)$. Hence, A is abelian.

The converse is trivial.

Q.E.D.

2.4. Definition: A subautomaton B of an automaton $A = (Q, I, \delta)$ is said to be a primary of A if, and only if, the following two conditions are satisfied:

- (i) there exists $q \in Q$, such that $B = A(q)$;
- (ii) for all $p \in Q$, $B \ll A(p) \implies B = A(p)$.

Thus, a primary is a maximal subautomaton generated by a single state. We now show that the set of primaries of an automaton is both exhaustive and unique.

2.5. Primary Decomposition Theorem: Let $\mathbf{P} = \{P_1, \dots, P_n\}$ be the set of (distinct) primaries of an automaton $A = (Q, I, \delta)$. Then,

- (i) $A = \bigcup_{i=1}^n P_i$;
- (ii) $A \neq \bigcup_{i \neq j} P_i$, for any $j \in \{1, 2, \dots, n\}$.

Proof: (i) Let $q_0 \in Q$, and suppose that, for all $x \in I$ and for all $q \in Q - \delta_0(q_0)$, $\delta(q, x) \neq q_0$. Then, by # 2.4, $A(q_0)$ is a primary of A . Thus, suppose that, for some $x \in I$ and for some $q_1 \in Q - \delta_0(q_0)$, $\delta(q_1, x) = q_0$. Then, $\delta_0(q_0) \subsetneq \delta_0(q_1) \implies \#[\delta_0(q_0)] < \#[\delta_0(q_1)]$. If $A(q_1)$ is not a primary of A , there exist $x \in I$ and $q_2 \in Q - \delta_0(q_1)$, such that $\delta(q_2, x) = q_1$. Then, $\delta_0(q_0) \subsetneq \delta_0(q_1) \subsetneq \delta_0(q_2) \implies \#[\delta_0(q_0)] < \#[\delta_0(q_1)] < \#[\delta_0(q_2)]$. Since Q is finite, there exists $q_m \in Q$ such that, $q \in \delta_0(q_m)$ and $\delta(r, x) \neq q_m$, for all $r \in Q - \delta_0(q_m)$ and for all $x \in I$. Hence, for all $s \in Q$, $A(q_m) << A(s) \implies A(q_m) = A(s)$; i.e., $A(q_m)$ is a primary of A and, hence, is one of the P_i 's in $\mathbf{P}$. Thus, $A = \bigcup_{i=1}^n P_i$.

(ii) Let $B = \bigcup_{i \neq j} P_i$, and let $P_j = A(q)$, for some $j \in \{1, \dots, n\}$. We show that $q \notin Q_B$. Suppose $q \in Q_B$. Then, $q \in Q_{P_i}$ for some $i \neq j$. Let $P_i = A(p)$. Then, $q \in Q_{P_i} \implies$ by # 1.2 (iii), $\delta_0(q) \subseteq \delta_0(Q_{P_i}) = \delta_0(p) \implies A(q) << A(p) \implies$ by # 2.4 (ii), $A(q) = A(p) \implies P_i = P_j$, contradicting the hypothesis on $\mathbf{P}$. Thus, (ii) is proved.

We note that the same primary may have several generators, since $A(p) = A(q) \not\Rightarrow p = q$. Also, the same state may belong to more than one primary; i.e., distinct primaries may have a non-empty intersection.

2.6. Corollary: Let $\mathbf{P} = \{P_i: i = 1, 2, \dots, n\}$ be the set of primaries of an automaton A , and let $R = \{r_1, \dots, r_k\}$ be a minimal generating set of A . Then, $n = k$.

Proof: For each $P_i \in \mathbf{P}$, let $P_i = A(p_i)$. Then, by # 2.5 (i), since $\{p_1, p_2, \dots, p_n\}$ is a generating set, $k \leq n$, and by # 2.5 (ii), since each $A(r_j) \ll A(p_i)$ for some i , $n \leq k$.
Q.E.D.

2.7. Definition: The rank of an automaton A , denoted by $r(A)$, is defined as the number of distinct primaries of A (or the cardinality of any minimal generating set of A).

The primaries of an automaton are its natural major subdivisions. Many questions concerning automata may be answered, either largely or entirely, by investigating the primaries of the automata (as is done in following sections of this investigation). As an immediate illustration, we make use of primaries to characterize a retrievable automaton ([10], [11], [12], and [13]) as one whose primaries are strongly connected (and hence disjoint). An automaton $A = (Q, I, \delta)$ is said to be retrievable if, and only if, for each $x \in I$ and for each $q \in Q$, there exists a corresponding $y \in I$, such that $\delta(q, xy) = q$.

2.8. Theorem: An automaton is retrievable if, and only if, its primaries are strongly connected.

Proof: Suppose that all primaries of an automaton, A , are strongly connected, and let $q \in Q$, $x \in I$. By # 2.5, there exists a primary, $A(p)$, of A , such that $q \in \delta_0(p)$. Since $A(p)$ is strongly connected, there exists $y \in I$, such that $\delta[\delta(q, x), y] = \delta(q, xy) = q$, since $q \in \delta_0(p)$. Hence, $\delta(q, x) \in \delta_0(p)$ and, therefore, A is retrievable.

Conversely, let A be retrievable, let $A(p)$ be a primary of A , and let $q \in \delta_0(p)$. A is retrievable $\implies$ by # 1.2 (iv), $\delta_0(q) \subseteq \delta_0[\delta_0(p)] = \delta_0(p) \implies A(q) \ll A(p) \implies$ by # 2.4 (ii), $A(q) = A(p) \implies$ by # 1.8, $A(p)$ is strongly connected.

Q.E.D.

3. SOURCE

Another of the elementary building blocks of automata (and, indeed, of abstract algebras) is the "source". Intuitively, one may regard the source as a generalization of the notion of predecessors of a state of an automaton (alt., an element of an algebra).

3.1. Definition: Let $B = (P, I, \delta) \ll A = (Q, I, \delta)$, and let $R \subseteq P$. A state $p \in P$ is said to be an R-source in B if, and only if, there exists $x \in I$, such that $\delta(p, x) \in R$.

The source of R in B, denoted by $s(R; B)$, is defined by,

$$s(R; B) = \{p \in P: \delta(p, x) \in R, \text{ for some } x \in I^*\}.$$

The pure source of R in B, denoted by $s^-(R; B)$, is defined by,

$$s^-(R; B) = \{p \in P: \delta(p, x) \in R, \text{ for some } x \in I\}.$$

The pure source of R may, but need not, include all elements of R . The source of R , however, includes all elements of R . When the automaton, A , in which the source is taken, is evident and no ambiguity may arise, we may use $s(R)$ for $s(R; A)$, and $s^-(R)$ for $s^-(R; A)$.

We note that $s^-(R; B)$ is the set of all R -sources in B , while

$$s(R; B) = s^-(R; B) \cup R,$$

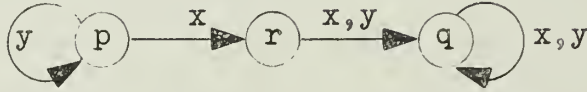
since $s(R; B)$ allows predecessors by the empty input. It is, then, trivially true that,

$$s^-(R; B) \subseteq s(R; B),$$

and that

$$R \subseteq s(R; B).$$

The reverse inclusions, however, do not hold, as can be seen from the following example:



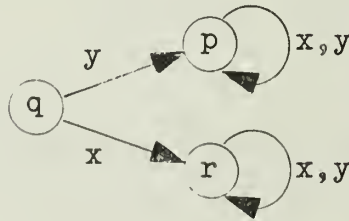
Here, if $R = \{r\}$, then $s(R) = \{p, r\}$ and $s^-(R) = \{p\}$. From the definition # 3.1 and the above example, it is also clear that, where R is an arbitrary subset of the set of states of an automaton, we may have

$$R \not\subseteq \delta[s^-(R; B)] \subsetneq \delta[s(R; B)],$$

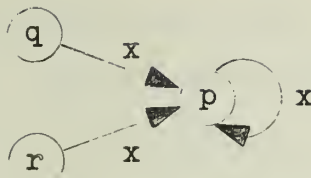
as is seen in the above example when $R = \{r\}$ and $Q_B = \{r, q\}$, and

$$R \not\subseteq s^-(R; B) \subsetneq s(R; B) \subsetneq s[\delta(R); B],$$

as is seen in the above example when $R = \{r\}$ and $Q_B = \{p, r, q\}$. Furthermore, neither of $s[\delta_0(R); B]$ and $\delta_0[s(R; B)]$ need be contained in the other, as may be seen from the following examples.



Let $R = \{r\}$, and let $Q_B = \{p, q, r\}$. Then, $s[\delta_0(R); B] = \{q, r\}$, and $\delta_0[s(R; B)] = \{p, q, r\}$.



Let $R = \{r\}$, and let $Q_B = \{p, q, r\}$. Then, $s[\delta_0(R); B] = \{p, q, r\}$, and $\delta_0[s(R; B)] = \{r, p\}$.

However, as may be seen from lemma # 3.3, below, more can be said when $(R, I, \delta) \ll A$. First, though, we state a few elementary results concerning the source, leaving the corresponding results concerning the pure source as a simple exercise.

3.2. Lemma: Let $B_1, B_2, \dots, B_n$ be arbitrary subsets of Q , where $A = (Q, I, \delta)$. Then,

- (i) $s(\bigcup_{i=1}^n B_i) = \bigcup_{i=1}^n s(B_i)$.
- (ii) $s(\bigcap_{i=1}^n B_i) \subseteq \bigcap_{i=1}^n s(B_i)$.
- (iii) $s(B_i) - s(B_j) \subseteq s(B_i - B_j)$, for all $i, j \in \{1, \dots, n\}$.
- (iv) $-s(B_j) \subseteq s(-B_j)$, for all j .
- (v) $s(s(\dots s(B_1) \dots)) = s(B_1)$, for all i .
- (vi) $\delta_0(B_i) \cap B_j = \emptyset \iff B_i \cap s(B_j) = \emptyset$, for all i, j .
- (vii) $B_i \subseteq B_j \implies s(B_i) \subseteq s(B_j)$, for all i, j .

Proof: (i) $q \in s(B_i \cup B_j) \iff$ there exists $x \in I^*$, such that $\delta(q, x) \in B_i \cup B_j \iff \delta(q, x) \in B_i$ or $\delta(q, x) \in B_j \iff q \in s(B_i)$ or $q \in s(B_j) \iff q \in s(B_i) \cup s(B_j)$. The result, then, follows by induction.

(ii) $q \in s(B_i \cap B_j) \implies$ there exists $x \in I^*$, such that $\delta(q, x) \in B_i \cap B_j \implies \delta(q, x) \in B_i$ and $\delta(q, x) \in B_j \implies q \in s(B_i)$ and $q \in s(B_j) \implies q \in s(B_i) \cap s(B_j)$. The result, then, follows by induction.

(iii) $q \in s(B_i) - s(B_j) \implies \delta_0(q) \cap B_j = \emptyset$ and there exists $x \in I^*$, such that $\delta(q, x) \in B_i \implies \delta(q, x) \in B_i - B_j \implies q \in s(B_i - B_j)$.

(iv) This result follows from (iii) when $B_i = Q$.

(v) Trivially, $s(s(B_i)) = s(B_i)$. The result, then, follows by induction.

(vi) This result follows directly from the definition.

(vii) This result follows directly from the definition.

Q.E.D.

It is easily seen that the inclusion in each of (ii), (iii), and (iv) of # 3.2 may not be replaced by an equality.

3.3. Lemma: Let $C = (R, I, \delta) \ll B \ll A$. Then,

(i) $R \subseteq s^-(R; B)$.

(ii) $s^-(R; B) = s(R; B) = s[\delta_0(R); B] = s[\delta(R); B]$.

(iii) $\delta[s^-(R; B)] = \delta[s(R; B)]$.

(iv) $s[\delta_0(R); B] \subseteq \delta_0[s(R; B)]$.

Proof: Let $r \in R$. Then, $C \ll B \implies \delta(r) \subseteq R \implies$ there exists $x \in I$, such that $\delta(r, x) \in R \implies r \in s^-(R; B) \implies R \subseteq s^-(R; B)$, and (i) is proved.

The first equality in (ii) follows from (i) and the definition # 3.1, since $s(R; B) = s^-(R; B) \cup R$. The second

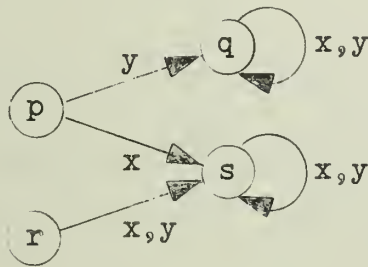
equality follows from the fact that $C \ll B \implies R = \delta_0(R)$. To prove the third equality, we note that, by # 3.2 (vii), $\delta(R) \subseteq \delta_0(R) \implies s[\delta(R); B] \subseteq s[\delta_0(R); B]$. Conversely, $s(R; B) \subseteq s[\delta(R); B]$ and hence, by the second equality of (ii), $s[\delta_0(R); B] \subseteq s[\delta(R); B]$. The two inclusions prove the third equality, which concludes the proof of (ii).

The equality in (iii) is immediate from the first equality of (ii).

The inclusion in (iv) is immediate from the second equality in (ii) and definition # 1.1.

Q.E.D.

We note that the inclusion in (iv) cannot be strengthened to an equality, even in the two cases where B on the one hand, or (R, I, δ) on the other, is a primary. The former is evident from the first of the two examples preceding # 3.2. To demonstrate the latter case, let $A = (Q, I, \delta)$, with $Q = \{p, q, r, s\}$, $M = \{x, y\}$, $\delta(r, x) = \delta(r, y) = \delta(s, x) = \delta(s, y) = \delta(p, x) = s$, and $\delta(p, y) = \delta(q, x) = \delta(q, y) = q$.



Let $R = \{r, s\}$, and let $B = A$. Then, $s[\delta_0(R); B] = \{p, r, s\}$, while $\delta_0[s(R; B)] = \{p, q, r, s\}$.

It is of interest to note that the source and the minimal automaton of a state, q , are complementary opposites, in that the former contains all predecessors of q , but not necessarily its successors, while the latter contains all successors of q , but not necessarily its predecessors. Often, a combination of the two concepts suffices to characterize a property of automata, such as: $A[s(q)]$ is the union of all primaries in which q is a state. As another illustration, we present a necessary condition for an automaton to be abelian.

3.4. Theorem: In an abelian automaton, disjoint subautomata have disjoint sources.

Proof: Let $B \ll A$, $C \ll A$, and $Q_B \cap Q_C = \emptyset$, and suppose there exists $q \in s(B) \cap s(C)$. Then, there exist $x, y \in I^*$, such that $\delta(q, x) \in Q_B$ and $\delta(q, y) \in Q_C$. But then, $B \ll A \implies \delta(q, xy) = \delta[\delta(q, x), y] \in Q_B$, and $C \ll A \implies \delta(q, yx) \in Q_C$. But, $Q_B \cap Q_C = \emptyset \implies \delta(q, xy) \neq \delta(q, yx)$ and, hence, A is not abelian. Thus, if A is abelian, then $Q_B \cap Q_C = \emptyset \implies s(B) \cap s(C) = \emptyset$.

Q.E.D.

In terms of the notation of section # 1, $(P, I, \delta) \ll A$ if, and only if, $\delta_0(P) = P$. We now characterize subautomata by means of the source.

3.5. Theorem: For all $P \subseteq Q$, where $A = (Q, I, \delta)$, $\delta_0(P) = P$ if, and only if, $s(\{q\}) \cap P \neq \emptyset \implies q \in P$, for any $q \in Q$.

Proof: Suppose $s(\{q\}) \cap P \neq \emptyset \implies q \in P$. By # 3.2 (vi), $s(\{q\}) \cap P \neq \emptyset \iff \{q\} \cap \delta_0(P) \neq \emptyset \iff q \in \delta_0(P)$. Hence, $q \in \delta_0(P) \implies q \in P$ and, thus, $\delta_0(P) \subseteq P$. Since, by # 1.1, the reverse inclusion is always true, $\delta_0(P) = P$.

Conversely, let $\delta_0(P) = P$, and suppose $s(\{q\}) \cap P \neq \emptyset$. Then, by # 3.2 (vi), $\{q\} \cap \delta_0(P) \neq \emptyset$ and, hence, $q \in \delta_0(P) = P$.

Q.E.D.

In terms of the notation of section # 1, a subautomaton, $B = (P, I, \delta)$, of A is strongly connected if, and only if, for all non-empty $R \subseteq P$, $\delta(R) = P$. We now characterize strongly connected subautomata by means of the source.

3.6. Theorem: Let $B = (P, I, \delta) \ll A$. Then, B is strongly connected if, and only if, for all non-empty $R \subseteq P$, $s(R; B) = P$.

Proof: Suppose, for all non-empty $R \subseteq P$, $s(R; B) = P$, and let $p, q \in P$. Then, $\{p\} \subseteq s(\{p\}; B) = P = s(\{q\}; B) \implies$ there exists $x \in I^*$, such that $\delta(p, x) = q$. Hence, B is strongly connected.

Conversely, suppose B is strongly connected, and let R be a non-empty subset of P . Then, for any $p \in P$, there exists $x \in I$, such that $\delta(p, x) \in R \implies P \subseteq s(R; B) \implies P = s(R; B)$.

Q.E.D.

We note that theorems ## 3.5 and 3.6 generalize to monadic algebras without change in either statement or proof.

Trivially, since $Q = s(Q)$, the set of states of an automaton is the union of the sources of all its subautomata. We now show that the strongly connected subautomata are sufficient for this purpose.

3.7. Theorem: Let $B_1, B_2, \dots, B_n$ be all the strongly connected subautomata of A . Then, $Q = \bigcup_{i=1}^n s(Q_{B_i})$.

Proof: Let $q \in Q - \bigcup_{i=1}^n s(Q_{B_i})$. Then, by # 3.2 (i) and (vi), $q \notin s(\bigcup_{i=1}^n Q_{B_i}) \implies \delta_0(q) \cap (\bigcup_{i=1}^n Q_{B_i}) = \emptyset$. But, $A(q) \ll A \implies$ there exists a strongly connected subautomaton $C \ll A(q)$, by # 1.7, and, hence, $Q_C \cap (\bigcup_{i=1}^n Q_{B_i}) = \emptyset$, contradicting the hypothesis that $B_1, B_2, \dots, B_n$ are all the strongly connected subautomata of A . Hence, $Q = \bigcup_{i=1}^n s(Q_{B_i})$.

Q.E.D.

We call a subautomaton (alt., subalgebra), $B = (P, I, \delta)$, of A separated if, and only if, $\delta_0(Q - P) \cap P = \emptyset$. We call an automaton (alt., algebra) discrete if, and only if, each of its states (alt., elements) is a (separated) subautomaton (alt., subalgebra) of A ; i.e., for all $q \in Q$, $\delta_0(q) = \{q\}$. In that case, $\#(Q) = r(A)$ and each primary of A has exactly one state (see definition # 2.7). Indeed, a discrete algebra is of little interest in itself; it does, however, represent the opposite of a strongly connected algebra.

We conclude this section with several characterizations of automata and algebras, which make use of the concept of source.

3.8. Theorem: Let $P \subseteq Q$, where $A = (Q, I, \delta)$. Then,

(i) where $B = (P, I, \delta) \ll A$, $P = s(P)$ if, and only if, B is separated;

(ii) $P_i = s(P_i)$ for all $B_i = (P_i, I, \delta) \ll A$ if, and only if, A is retrievable (see # 2.8 and [10]);

(iii) $P = s(P)$, for all $P \subseteq Q$, if, and only if, A is discrete.

Proof: (i) Let $B = (P, I, \delta) \ll A$, and suppose $P = s(P)$. Then, $\emptyset = (Q - P) \cap P = (Q - P) \cap s(P) \implies \delta_0(Q - P) \cap P = \emptyset$, by # 3.2 (vi), and B is separated.

Conversely, suppose B is separated. Then, $\delta_0(Q - P) \cap P = \emptyset \implies$ by # 3.2 (vi), $(Q - P) \cap s(P) = \emptyset \implies P = P \cup [(Q - P) \cap s(P)] = [P \cup (Q - P)] \cap [P \cup s(P)] = Q \cap s(P) = s(P)$.

(ii) Let $P_i = s(P_i)$, for all $B_i = (P_i, I, \delta) \ll A$. Let $x \in I$, $q \in P_i$ for some i , and suppose $\delta(q, xy) \neq q$, for all $y \in I^*$. Then, $q \notin \delta_0[\delta(q, x)]$ and, hence, $q \in s(\delta_0[\delta(q, x)]) - \delta_0[\delta(q, x)]$. But, $\delta_0[\delta(q, x)]$ is the set of states of $A[\delta(q, x)] \ll A$, contradicting the hypothesis. Hence, A is retrievable.

Conversely, let A be retrievable. Then, by # 2.8, A is the (disjoint) union of strongly connected subautomata. But, by # 1.8, a strongly connected automaton has no proper sub-

automaton and, hence, $P_1 = s(P_1)$ for all subautomata $B_1 = (P_1, I, \delta)$ of A .

(iii) Let $P = s(P)$, for all $P \subseteq Q$. Suppose there exist $q \in Q$ and $x \in I$, such that $\delta(q, x) = p \neq q$. Then, $q \in s(\{p\}) \implies \{p\} \neq s(\{p\})$, contradicting the hypothesis. Hence, for all $q \in Q$, $\delta_0(q) = \{q\}$ and A is discrete.

The converse is trivial.

Q.E.D.

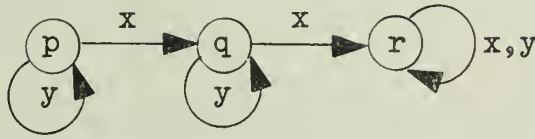
3.9. Remark: Bavel and Muller ([10], definition 1) define eight reversibility properties of monadic algebras, with $k_1(A)$, or its abbreviation k_1 , being the statement that algebra A possesses property 1, where property $i \in \{1, 2, \dots, 8\}$ is named: (1) semiretrievable, (2) retrievable, (3) unique predecessor, (4) onto, (5) partially reversible, (6) potentially reversible, (7) reversible, and (8) strongly connected. If we let $k_9(A)$ be the statement that algebra A is discrete, it is easily verifiable that $k_9 \implies k_7$.

We now define an additional reversibility property for monadic algebras and present equivalent formulations which employ the source.

3.10. Definition: An algebra $A = (Q, I, \delta)$ is said to be reflexive if, and only if, for each $q \in Q$ there exists $x \in I$, such that $\delta(q, x) = q$.

We let $k_{10}(A)$ be the statement that algebra A is reflexive.

From the following example, it is easily seen that $k_{10} \not\Rightarrow k_1$, $i \in \{1, 2, \dots, 9\}$: Let $A = (Q, M, \delta)$, with $Q = \{p, q, r\}$, $M = \{x, y\}$, $\delta(p, y) = p$, $\delta(p, x) = \delta(q, y) = q$, and $\delta(q, x) = \delta(r, x) = \delta(r, y) = r$.



3.11. Theorem: The following statements are equivalent for the algebra $A = (Q, M, \delta)$:

(i) A is reflexive.

For all $R \subseteq Q$, for all $B \ll A$,

(ii) $R \subseteq Q_B \Rightarrow R \subseteq s^-(R; B)$.

(iii) $R \subseteq Q_B \Rightarrow R \subseteq \delta[s^-(R; B)]$.

(iv) $(R, I, \delta) \ll B \Rightarrow R \subseteq \delta[s^-(R; B)]$.

Proof: (i) $\Rightarrow$ (ii): Let $q \in R \subseteq Q_B$. Then, $k_{10} \Rightarrow$ there exists $x \in I$, such that $\delta(q, x) = q \Rightarrow q \in s^-(\{q\}; B) \Rightarrow q \in s^-(R; B) \Rightarrow R \subseteq s^-(R; B)$.

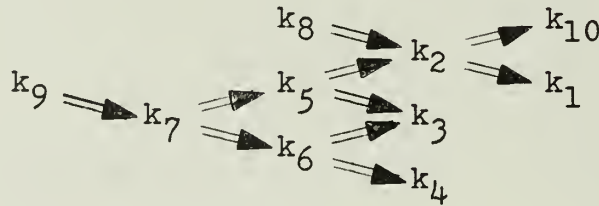
(ii) $\Rightarrow$ (iii): $R \subseteq s^-(R; B) \Rightarrow$ for each $r \in R$ there exists $x \in I$, such that $\delta(r, x) \in R \Rightarrow R \subseteq \delta(R)$. But, $R \subseteq s^-(R; B) \Rightarrow \delta(R) \subseteq \delta[s^-(R; B)]$, by # 1.2 (iii). Hence, $R \subseteq \delta(R) \subseteq \delta[s^-(R; B)]$.

(iii) $\Rightarrow$ (iv): This is immediate, since $(R, I, \delta) \ll B \Rightarrow R \subseteq Q_B$.

(iv) $\implies$ (i): Suppose $(R, I, \delta) \ll B \implies R \subseteq \delta[s^-(R; B)]$ for all $B \ll A$, and let $q \in Q_B$. Then, since $A(q) \ll A(q)$, by hypothesis, $\delta_0(q) \subseteq \delta[s^-(\delta_0(q); A(q))] \implies q \in \delta[s^-(\delta_0(q); A(q))] \implies$ there exist $p \in s^-(\delta_0(q); A(q))$ and $x \in I$, such that $q = \delta(p, x)$. But, $p \in s^-(\delta_0(q); A(q)) \implies p \in \delta_0(q) \implies$ there exists $y \in I^*$, such that $\delta(q, y) = p$. Hence, $q = \delta(p, x) = \delta[\delta(q, y), x] = \delta(q, yx)$, and A is reflexive.

Q.E.D.

It is easily verifiable that $k_2 \implies k_{10}$; i.e., a retrievable algebra is reflexive. Thus, we may amplify a consequence of theorem 1 in [10] to read: The following graph shows the implication relations between pairs of properties $k_1, \dots, k_{10}$:



Two of the reversibility properties, k_2 and k_8 , mentioned in # 3.9, were characterized in ## 3.8 (ii) and 3.6, respectively, by means of the source. The remaining six properties may be similarly characterized, using the source as it applies to particular members of I ; i.e., $s_x(P; B) = \{q \in Q_B: \delta(q, x^n) \in P, n \text{ is an integer } \geq 0\}$, and $s_x^-(P; B) = \{q \in Q_B: \delta(q, x^n) \in P, n \text{ is an integer } > 0\}$. However, we omit the details, as this would constitute too much of a digression.

4. HOMOMORPHISMS AND SOURCE

4.1. Definition:⁽⁴⁾ Let $A = (Q, I, \delta)$ and $B = (Q^0, I, \delta^0)$ be two automata. By a function, $f: A \longrightarrow B$, on A to B is meant a function $f: Q \longrightarrow Q^0$. A function, $f: A \longrightarrow B$, is called a homomorphism⁽⁵⁾ if, and only if, for all $q \in Q$ and for all $x \in I$, $f[\delta(q, x)] = \delta^0[f(q), x]$. By the homomorphic image, $f(A)$, of A under the homomorphism $f: A \longrightarrow B$ is meant the subautomaton $f(A) = (f(Q), I, \delta^0) \ll B$, where $f(Q)$ is the set of images of Q under f . Following the common practice, we call a homomorphism, $f: A \longrightarrow B$, an endomorphism of A , when $B = A$; an isomorphism of A , when f is monic (i.e., one-to-one) and epic (i.e., onto); an automorphism of A , when f is an isomorphism of A onto A . By $G(A)$ we denote the group of automorphisms of A .

4.2. Remark: The homomorphic image, $f(A)$, of an automaton $A = (Q, I, \delta)$ is, indeed, a subautomaton; i.e., $f(Q)$ is closed under δ^0 . For, if $p \in f(Q)$, then there exists $q \in Q$, such that $p = f(q)$ and, hence, for any $x \in I$, $\delta^0(p, x) = \delta^0[f(q), x] = f[\delta(q, x)] \in f(Q)$.

The set of all automorphisms of A is (trivially) a

(4)

Parts of this definition parallel those of Fleck [5], Weeg [7], and Gluschkov [13].

(5)

Fleck [5] and Weeg [7] call a homomorphism an "operation preserving function."

group under functional composition.⁽⁶⁾

In this investigation, we are primarily concerned with the automorphisms of an automaton. Nevertheless, when we think it appropriate, we present results of a more general nature, concerning homomorphisms, endomorphisms, and isomorphisms of automata.

4.3. Lemma: Let f be a homomorphism on A , let $B \ll A$, and let $P \subseteq Q_B$. Then,

- (i) $f[s^-(P; B)] \subseteq s^-[f(P); f(B)]$;
- (ii) $f[s(P; B)] \subseteq s[f(P); f(B)]$.

Proof: Let $q \in s^-(P; B)$. Then, there exists $x \in I$, such that $\delta(q, x) \in P \implies f[\delta(q, x)] = \delta'[f(q), x] \in f(P) \subseteq f(Q_B) \implies f(q) \in s^-[f(P); f(B)] \implies f[s^-(P; B)] \subseteq s^-[f(P); f(B)]$.

This proves (i).

Using (i) and $s(P; B) = P \cup s^-(P; B)$ we have, $f[s(P; B)] = f(P) \cup f[s^-(P; B)] \subseteq f(P) \cup s^-[f(P); f(B)] = s[f(P); f(B)]$. This proves (ii).

Q.E.D.

We combine lemma # 4.3 and the characterization of strongly connected subautomata in theorem # 3.6 to prove:

(6) This fact has been noted by Fleck ([5], theorem 1). Weeg ([7], theorem A) attributes to Fleck the result: The set of all endomorphisms on A is a group. However, as there is a discrepancy between the range and domain of composed endomorphisms, this result does not hold, except when A is strongly connected (see # 4.8, below).

4.4. Theorem: The homomorphic image of a strongly connected subautomaton is strongly connected.

Proof: Let $B = (P, I, \delta) \ll A$ be strongly connected, let f be a homomorphism on A , and let $\emptyset \neq R \subseteq f(P)$. Then, for some non-empty $T \subseteq P$, $f(T) = R$. By # 3.6, B is strongly connected $\implies P = s(T; B) \implies f(P) = f[s(T; B)] \subseteq s[f(T); f(B)]$, by # 4.3. But, $s[f(T); f(B)] = s[R; f(B)] \subseteq f(P) \implies f(P) = s[R; f(B)] \implies f(B)$ is strongly connected, by # 3.6.

Q.E.D.

It should be noted that theorem # 4.4 may be proved without making use of the source. We chose the more topical proof.

4.5. Theorem: Let $R \subseteq P$, where $B = (P, I, \delta) \ll A$, and let h be an isomorphism on A . Then,

- (i) $h[s(R; B)] = s[h(R); h(B)]$;
- (ii) $h[s(R; B) - R] = s[h(R); h(B)] - h(R)$.

Proof: (i) By lemma # 4.3, $h[s(R; B)] \subseteq s[h(R); h(B)]$ and it remains to show the converse.

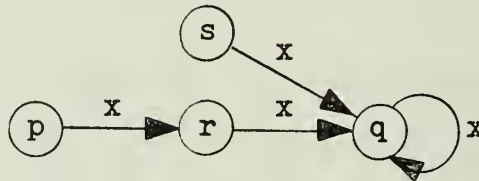
Let $q^0 \in s[h(R); h(B)]$. Then, there exists $x \in I^*$ and there exists $p^0 \in h(R)$, such that $\delta^0(q^0, x) = p^0$. Since h is monic, let $h^{-1}(q^0) = q$ and $h^{-1}(p^0) = p$. Then, $p^0 = h(p) = \delta^0[h(q), x] = h[\delta(q, x)] \implies p = \delta(q, x)$, where $p \in R$ and, hence, $q \in s(R; B)$. Thus, $q^0 \in h[s(R; B)]$ and, hence, $s[h(R); h(B)] \subseteq h[s(R; B)]$.

(ii) It is an elementary property of functions that, for any function f and any sets C and D , $f^{-1}[C - D] = f^{-1}[C] - f^{-1}[D]$ (for example, see Kelly [14], theorem 0.7). Since h is monic, let $f = h^{-1}$, let $C = s(R; B)$, and let $D = R$. Then, $h[s(R; B) - R] = h[s(R; B)] - h(R) = s[h(R); h(B)] - h(R)$, by (i).

Q.E.D.

4.6. Remark: In general, the equalities in # 4.5 (i) and (ii) do not hold if h is just a homomorphism.

Proof: Let $B = (Q, I, \delta)$, with $Q = \{p, q, r, s\}$, $M = \{x\}$, $\delta(p, x) = r$, and $\delta(r, x) = \delta(q, x) = \delta(s, x) = q$.



Let h be defined by, $h(p) = r$, $h(r) = h(q) = q$, and $h(s) = s$. Then, h is an endomorphism of B and $h(B) = (\{q, r, s\}, I, \delta)$. Now, where $R = \{r\}$, $s(R; B) = \{p, r\}$, $h[s(R; B)] = \{r, q\}$, $s[h(R); h(B)] = s[\{q\}; h(B)] = \{q, r, s\}$, $h[s(R; B) - R] = \{r\}$, and $s[h(R); h(B)] - h(R) = \{r, s\}$. Hence,

$$h[s(R; B)] \subsetneq s[h(R); h(B)],$$

and

$$h[s(R; B) - R] \subsetneq s[h(R); h(B)] - h(R).$$

Q.E.D.

4.7. Theorem: Let $f: A \rightarrow A$ be an endomorphism, let $B \ll A$ be strongly connected, and let $q \in Q_B$ be such that $f(q) \in Q_B$. Then, $f(B) = B$.

Proof: Since $f(q) \in Q_B \cap f(Q_B)$, the subautomaton $B \cap f(B)$ is non-empty. But, by # 4.4, $f(B)$ is strongly connected and, by # 1.8, neither B nor $f(B)$ have a proper subautomaton. Hence, $B \cap f(B) = B = f(B)$.

Q.E.D.

4.8. Corollary: any endomorphism, f , on a strongly connected automaton is an automorphism.

Proof: By # 4.7, f is epic and, since the set of states of an automaton is finite, f is monic.

Q.E.D.

4.9. Corollary: Let $h \in G(A)$ and suppose that, for some strongly connected $B \ll A$ and for some $q \in Q_B$, $h(q) \in Q_B$. Then, $h[s(Q_B)] = s(Q_B)$.

Proof: By # 4.7, $h(B) = B$; i.e., $h(Q_B) = Q_B$. Hence, by # 4.5, $h[s(Q_B)] = s[h(Q_B)] = s(Q_B)$.

Q.E.D.

4.10. Remark: The conclusion of # 4.9 does not follow if any of the following conditions applies: (i) h is a non-monic homomorphism, (ii) B is not strongly connected, (iii) the last condition in the corollary is changed to read, "for some q in

$s(Q_B) = Q_B$, $h(q) \in s(Q_B) = Q_B$."

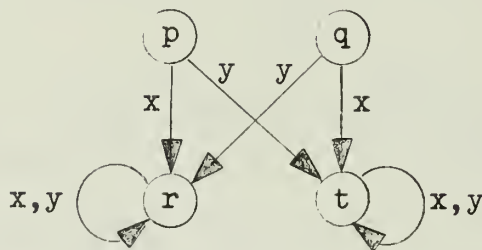
Proof: (i) This is immediate from the example in remark # 4.6, where $Q_B = \{q\}$.

(ii) Let $A = (Q, I, \delta)$, with $Q = \{p, q\}$, $M = \{x\}$, $\delta(p, x) = p$, $\delta(q, x) = q$, $h(p) = q$, and $h(q) = p$.



Then, $h \in G(A)$, yet $h[s(\{p\})] = h(\{p\}) = \{q\}$, while $s(\{p\}) = \{p\}$.

(iii) Let $A = (Q, I, \delta)$, with $Q = \{p, q, r, t\}$, $M = \{x, y\}$, $\delta(p, x) = \delta(q, y) = \delta(r, x) = \delta(r, y) = r$, $\delta(p, y) = \delta(q, x) = \delta(t, x) = \delta(t, y) = t$, $h(p) = q$, $h(q) = p$, $h(r) = t$, and $h(t) = r$.



Then, $h \in G(A)$. Let $Q_B = \{r\}$. Then, $s(Q_B) = \{p, q, r\}$, $h(p) = q \in s(Q_B)$, but $h[s(Q_B)] = \{q, p, t\} \neq \{p, q, r\} = s(Q_B)$.

Q.E.D.

In [7], Weeg states and proves in lemma 1: If G is a group of regular permutations on $\{0, 1, 2, \dots, n-1\}$ and if for some integer i in that set, $f(i) = g(i)$, for $f, g \in G$, then $f = g$. Fleck states and proves an analogous result as lemma 1 in [5]: If $A = (Q, I, \delta)$ is a strongly connected

automaton and f and g are endomorphisms⁽⁷⁾ of A , with $f(p) = g(p)$ for some $p \in Q$, then $f = g$ (i.e., $f(q) = g(q)$, for all $q \in Q$).

The following theorem # 4.11 and corollary # 4.12 are generalizations of these results to minimal automata and sources.

4.11. Theorem: Let $f, g: A = (Q, I, \delta) \longrightarrow A' = (Q', I, \delta')$ be homomorphisms, such that $f(q) = g(q)$, for some $q \in Q$. Then, $f = g$ on $A(q)$. If, furthermore, $q \in s(Q_B)$, where $B \ll A$ is strongly connected, then $f = g$ on B .

Proof: Let $p \in \delta_0(q)$, say, $p = \delta(q, x)$. Then, $f(p) = f[\delta(q, x)] = \delta'[f(q), x] = \delta'[g(q), x] = g[\delta(q, x)] = g(p)$.

The second part of the theorem is a trivial consequence of the first.

Q.E.D.

4.12. Corollary: Let f be an endomorphism of $A = (Q, I, \delta)$ such that, for some $q \in Q$, $f(q) = q$. Then, f is the identity on $A(q)$. If, furthermore, $q \in s(Q_B)$, where $B \ll A$ is strongly connected, then f is the identity on B .

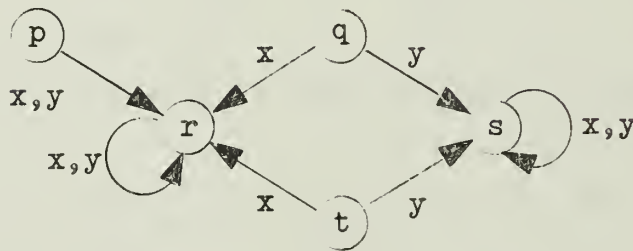
Proof: The corollary is immediate from # 4.11, with g taken as the identity automorphism on A .

Q.E.D.

⁽⁷⁾ By # 4.8, f and g are, then, automorphisms of A .

4.13. Remark: The conditions of # 4.12 are not sufficient for f to be the identity on $s(Q_B)$, even if $f \in G(A)$.

Proof: Consider the automaton $A = (Q, I, \delta)$, with $Q = \{p, q, r, s, t\}$; $M = \{x, y\}$; $\delta(p, x) = \delta(p, y) = \delta(r, x) = \delta(r, y) = \delta(q, x) = \delta(t, x) = r$, $\delta(q, y) = \delta(t, y) = \delta(s, x) = \delta(s, y) = y$; $h(p) = p$, $h(r) = r$, $h(s) = s$, $h(q) = t$, and $h(t) = q$.



Here, $p \in s(\{r\})$ and $h(p) = p$, where $h \in G(A)$. Yet, $q \in s(\{r\})$ and $h(q) = t \neq q$.

Q.E.D.

We conclude this section by showing that both of the reversibility properties, k_9 and k_{10} , defined in section # 3, are preserved under homomorphism (the interested reader will find a discussion of the homomorphic images of algebras possessing one of the remaining eight reversibility properties in [10]).

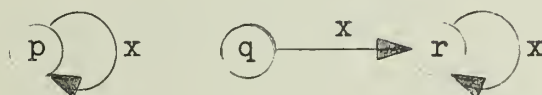
4.14. Theorem: The homomorphic image of a discrete algebra is discrete.

Proof: Let $A = (Q, I, \delta)$ be a discrete algebra, let $f: A \rightarrow A' = (Q', I, \delta')$ be a homomorphism, let $p' \in h(Q)$,

and let $q^0 \in s[\{p^0\}; h(A)]$. Then, there exists $x \in I^*$, such that $\delta^0(q^0, x) = p^0$. Let q and p be any states in Q , such that $h(q) = q^0$ and $h(p) = p^0$. Then, $s(\{q\}) = \{q\} \implies \delta(q, x) = q \implies q^0 = h(q) = h[\delta(q, x)] = \delta^0[h(q), x] = \delta^0(q^0, x) = p^0 \implies s[\{p^0\}; h(A)] = \{p^0\} \implies h(A)$ is discrete.

Q.E.D.

4.15. Remark: In contrast to # 4.14, the homomorphic image of a separated subautomaton need not be separated, as is seen from the following example. Let $Q = \{p, q, r\}$; $M = \{x\}$; $\delta(p, x) = p$, $\delta(q, x) = \delta(r, x) = r$; $f(p) = f(r) = r$, and $f(q) = q$.



Here, f is a homomorphism and $B = (\{p\}, I, \delta) \ll A$ is separated. Yet, $f(B) = (\{r\}, I, \delta)$, which is not separated.

4.16. Theorem: The homomorphic image of a reflexive algebra is reflexive.

Proof: Let $A = (Q, I, \delta)$ be reflexive, let $f: A \longrightarrow A^0$ be a homomorphism, and let $q^0 \in f(Q)$. Then, there exists $q \in Q$, such that $f(q) = q^0$, and there exists $x \in I$, such that $\delta(q, x) = q$. Hence, $q^0 = f(q) = f[\delta(q, x)] = \delta^0[f(q), x] = \delta^0(q^0, x)$ and, thus, $f(A)$ is reflexive.

Q.E.D.

5. MINIMAL AUTOMATA, CYCLES, AND AUTOMORPHISMS

In this section we characterize automorphisms of minimal automata with the aid of a new⁽⁸⁾ tool, -- the cycle.

5.1. Lemma: Let f be a homomorphism on $A = (Q, I, \delta)$ to $A' = (Q', I, \delta')$. Then, for each $q \in Q$, $f[A(q)] = A(f(q))$.

Proof: Since $f[\delta_0(q)] = f[\bigcup_{x \in I} \delta(q, x)] = \bigcup_{x \in I} f[\delta(q, x)] = \bigcup_{x \in I} \delta'[f(q), x] = \delta'_0[f(q)]$, we have $f[A(q)] = (f[\delta_0(q)], I, \delta') = (\delta'_0[f(q)], I, \delta') = A(f(q))$.

Q.E.D.

5.2. Theorem: Let $h \in G(A)$ and let $h(q) \in \delta_0(q)$, for some state q of A . Then, $h[A(q)] = A[h(q)] = A(q)$.⁽⁹⁾

Proof: The first equality is immediate from lemma # 5.1. Now, $h(q) \in \delta_0(q) \implies \delta_0[h(q)] \subseteq \delta_0[\delta_0(q)] = \delta_0(q)$, by # 1.2 (iii) and (iv). Hence, $h[\delta_0(q)] \subseteq \delta_0(q)$, by the first equality. But, since h is monic and $\delta_0(q)$ is finite, $h[\delta_0(q)] = \delta_0(q) \implies h[A(q)] = A(q) \implies A[h(q)] = A(q)$.

Q.E.D.

5.3. Definition: Let q be a state of $A = (Q, I, \delta)$ and let $x \in I$. Define $\delta(q, x^0) = \delta(q, \epsilon) = q$. Then,

⁽⁸⁾The reader should note that the "classical" use of the term "cycle" coincides with our "circular cycle" (see # 5.7).

⁽⁹⁾The reader may wish to compare # 5.2 with # 4.9.

the x-cycle of q , denoted by $C_x(q)$, is defined by,

$$C_x(q) = \{p \in Q: p = \delta(q, x^n), n = 0, 1, 2, \dots\}.$$

The length of the x-cycle of q is $\# [C_x(q)]$.

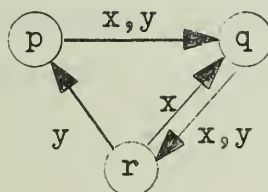
The reader will note that a cycle, as defined here, may be non-circular (see # 5.7, below).

5.4. Lemma: $\# [C_x(q)]$ = the least positive integer, n , for which there exists a non-negative integer $k < n$, such that $\delta(q, x^n) = \delta(q, x^k)$.

Proof: Let m be the least positive integer n for which there exists a non-negative integer $k < n$, such that $\delta(q, x^n) = \delta(q, x^k)$. Then, by a simple induction argument, for all non-negative integers r , $\delta(q, x^r) \in \{\delta(q, x^i): i = 0, 1, \dots, m-1\}$ and, hence, $\# [C_x(q)] \leq m$. But, since m is the least of the n 's, for any $s < m$, $\delta(q, x^{s+1}) \notin \{\delta(q, x^i): i = 0, 1, \dots, s\}$. Thus, $m \leq \# [C_x(q)]$. The two inequalities prove the lemma.

Q.E.D.

As an illustration, consider the automaton with $Q = \{p, q, r\}$, $M = \{x, y\}$, $\delta(p, x) = \delta(p, y) = \delta(r, x) = q$, $\delta(q, x) = \delta(q, y) = r$, and $\delta(r, y) = p$.



Here, $\#[C_X(p)] = \#\{p, q, r\} = 3$; $\#[C_X(q)] = \#\{q, r\} = \#[C_X(r)] = 2$; $\#[C_Y(p)] = \#[C_Y(q)] = \#[C_Y(r)] = \#\{p, q, r\} = 3$.

5.5. Theorem: Let f be a homomorphism on $A = (Q, I, \delta)$. Then, for any $q \in Q$ and for any $x \in I$,

- (1) $f[C_X(q)] = C_X[f(q)]$;
- (11) $\#(C_X[f(q)]) \leq \#[C_X(q)]$.

Proof: (1) $f[C_X(q)] = f[\{\delta(q, x^n) : n = 0, 1, 2, \dots\}] = \{f[\delta(q, x^n)] : n = 0, 1, 2, \dots\} = \{\delta^0[f(q), x^n] : n = 0, 1, 2, \dots\} = C_X[f(q)]$.

(11) By # 5.4, $\#[C_X(q)] =$ the least positive integer, n , such that, for some non-negative integer $k < n$, $\delta(q, x^n) = \delta(q, x^k)$. Hence, $\delta^0[f(q), x^n] = f[\delta(q, x^n)] = f[\delta(q, x^k)] = \delta^0[f(q), x^k] \implies \#(C_X[f(q)]) \leq n = \#[C_X(q)]$.

Q.E.D.

5.6. Corollary: Let $h \in G(A)$. Then, for any $q \in Q$ and for any $x \in I$, $\#[C_X(q)] = \#(C_X[h(q)])$.

Proof: The corollary is immediate from # 5.5 (1) and the fact that h is monic.

Q.E.D.

5.7. Definition: Let $q \in Q$ and $x \in I$, where $A = (Q, I, \delta)$. $C_X(q)$ is said to be circular if, and only if, $\delta(q, x^{\#[C_X(q)]}) = q$.

In the example following definition # 5.3, $C_y(p)$, $C_y(q)$, $C_y(r)$, $C_x(q)$, and $C_x(r)$ are circular; but $C_x(p)$ is not, since $\delta(p, x^3) = q \neq p$.

5.8. Lemma: Let f be an endomorphism on $A = (Q, I, \delta)$, and suppose for some $q \in Q$ and $x \in I$, $f(q) = \delta(q, x)$. Then, $f^n(q) = \delta(q, x^n)$, for all positive integers n .

Proof: The lemma clearly holds for $n = 1$. Suppose that $f^k(q) = \delta(q, x^k)$, for some positive integer k . Then, $f^{k+1}(q) = f[f^k(q)] = f[\delta(q, x^k)] = \delta[f(q), x^k] = \delta[\delta(q, x), x^k] = \delta(q, xx^k) = \delta(q, x^{k+1})$. Thus, the lemma follows by induction.

Q.E.D.

5.9. Definition: Let f be an endomorphism on $A = (Q, I, \delta)$. For each $q \in Q$, the f -cycle of q , denoted by $c_f(q)$, is defined by,

$$c_f(q) = \{f^n(q) : n = 0, 1, 2, \dots\},$$

where $f^0(q) \stackrel{\text{def}}{=} q$. The length of the f -cycle of q is $\# [c_f(q)]$.

We say that $c_f(q)$ is circular if, and only if,

$$f^{\# [c_f(q)]}(q) = q.$$

We note that, for any $q \in Q$, $\# [c_f(q)] > 0$, just as, for any $x \in I$, $\# [C_x(q)] > 0$. Furthermore, under the conditions of # 5.8, $c_f(q) = C_x(q)$. Indeed, this is a restatement of # 5.8 in terms of definition # 5.9, and we shall use the two statements interchangeably.

5.10. Lemma: $\#[c_f(q)]$ = the least positive integer, n , for which there exists a non-negative integer $k < n$, such that $f^n(q) = f^k(q)$.

Proof: The proof of the lemma is almost identical to that of # 5.4 and, therefore, we omit it.

Q.E.D.

5.11. Theorem: Let $h \in G(A)$. Then, $c_h(q)$ is circular for any state q of A .

Proof: Suppose $c_h(q)$ is not circular, and let $\#[c_h(q)] = n$. Then, $h^n(q) = p \neq q$. But, $p \in c_h(q) \implies$ there exists a least positive integer $k < n$, such that $h^n(q) = p = h^k(q) \implies$ by # 5.10, $h^{n-1}(q) \neq h^{k-1}(q)$. But then, two distinct states, $h^{n-1}(q)$ and $h^{k-1}(q)$, have the same value, p , under h . Hence, h is not monic, contradicting the hypothesis. Thus, $c_h(q)$ is circular.

Q.E.D.

5.12. Corollary: (i) Let $A = (Q, I, \delta)$, let $h \in G(A)$, and let $h(q) = \delta(q, x)$, for some $q \in Q$ and $x \in I$. Then, $C_x(q)$ is circular.

(ii) Let $h \in G[A(q)]$ be non-trivial (i.e., not the identity automorphism). Then, there exists $x \in I$, such that $h(q) = \delta(q, x)$, and $C_x(q)$ is circular.

(iii) Let $h \in G[A(q_0)]$ be non-trivial, with $\#[c_h(q_0)] = n$. Then, there exist distinct $q_1, q_2, \dots, q_n = q_0$ in

$\delta_0(q_0)$ and $x \in I$, such that $\delta(q_i, x) = q_{i+1}$ and $C_x(q_i)$ is circular with $C_x(q_i) = C_x(q_0)$, for each $i \in \{0, 1, \dots, n-1\}$.

Proof: (i) By # 5.8, $C_x(q) = c_h(q)$ and, hence, by # 5.11, $C_x(q)$ is circular.

(ii) Since h is non-trivial, $q \neq h(q) \in \delta(q)$. Hence, there exists $x \in I$, such that $h(q) = \delta(q, x)$. It follows from (i) that $C_x(q)$ is circular.

(iii) This is immediate from (ii) and # 5.8.

Q.E.D.

5.13. Lemma: Let $h \in G[A(q)]$. Then, h is completely determined by its value on q .

Proof: Let $p \in \delta_0(q)$. Then, there exists $x \in I^*$, such that $p = \delta(q, x)$. Since h is monic, we lose no generality by considering this representation of p , though others exist. Then, $h(p) = h[\delta(q, x)] = \delta[h(q), x]$ and, hence, $h(p)$ is determined by the value $h(q)$ on q .

Q.E.D.

We shall use the above lemma # 5.13 implicitly in the following discussion.

5.14. Theorem: Let q be a state of A . A necessary and sufficient condition for the existence of a non-trivial automorphism on $A(q)$ is the existence in A of a state $p \neq q$,

which satisfies:

$$(i) A(p) = A(q);$$

$$(ii) C_x(q) \text{ is circular, where } p = \delta(q, x);$$

$$(iii) \delta(q, y) = \delta(q, z) \implies \delta(p, y) = \delta(p, z), \text{ for any } y \text{ and } z \text{ in } I.$$

Proof of necessity: Let $h \in G[A(q)]$ be non-trivial. Then, by # 4.12 (or # 5.13), $h(q) \neq q$. Let $h(q) = p = \delta(q, x)$, since $h \in G[A(q)]$. Then, $q \neq h(q) \in A(q) \implies$ there exists $x \in I$, such that $\delta(q, x) = p$. By # 5.2, $A(p) = A[h(q)] = A(q)$ and, hence, $p \in \text{gen } A(q)$ and (i) is satisfied.

By # 5.12, $C_x(q)$ is circular and, thus, (ii) is satisfied.

Let $\delta(q, y) = \delta(q, z)$, for some $y, z \in I$. Then, $h[\delta(q, y)] = h[\delta(q, z)] \implies \delta[h(q), y] = \delta[h(q), z] \implies \delta(p, y) = \delta(p, z)$, and (iii) is satisfied.

Proof of sufficiency: Let (i), (ii), and (iii) be satisfied and define a function $h: A(q) \longrightarrow A(q)$ by,

$$h[\delta(q, u)] = \delta(p, u), \text{ for all } u \in I.$$

Now, suppose $\delta(q, u) = \delta(q, v)$, for some $v \in I$. Then, by (iii), $\delta(p, u) = \delta(p, v)$, so that $h[\delta(q, u)] = h[\delta(q, v)]$ and, thus, h is well defined on $A(q)$.

Let $\# [C_x(p)] = n$. Since $p \in C_x(q)$, $C_x(q) = C_x(p)$. Then, since $C_x(q)$ is circular by (ii), $h(q) = h[\delta(q, x^n)] = \delta(p, x^n) = p \neq q$, by # 5.12 (iii), and, hence, h is non-trivial.

Let $r = \delta(q, u)$ be an arbitrary state of $A(q)$. Then,

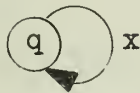
for any $v \in I$, $h[\delta(r, v)] = h(\delta[\delta(q, u), v]) = h[\delta(q, uv)] = \delta(p, uv) = \delta[\delta(p, u), v] = \delta(h[\delta(q, u)], v) = \delta[h(r), v]$. Hence, h is an endomorphism.

Now, let $r = \delta(q, u)$ and $s = \delta(q, v)$ be two states of $A(q)$, such that $h(r) = h(s)$. Then, $h^n(r) = h^n(s) \implies h^n[\delta(q, u)] = h^n[\delta(q, v)] \implies \delta[h^n(q), u] = \delta[h^n(q), v]$, since, if h is an endomorphism, so is h^n . But then, by # 5.8, $\delta[\delta(q, x^n), u] = \delta[\delta(q, x^n), v] \implies \delta(q, u) = \delta(q, v)$, since $\# [C_x(q)] = n$. I.e., $r = s$ and, therefore, h is monic. But, on a finite set, a monic endomorphism is epic and, thus, since $Q_{A(q)}$ is finite, h is epic. Hence, h is an automorphism.

Q.E.D.

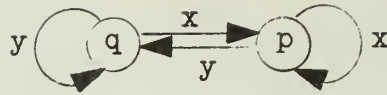
The following examples satisfy all conditions of # 5.14, save one, but not its conclusion. We note that, if $C_x(q)$ is circular, then $\delta(q, x) \in \text{gen } A(q)$, so that an example separating these two conditions cannot be given,

(a) Let A be the trivial automaton; i.e., $Q = \{q\}$, $M = \{x\}$, and $\delta(q, x) = q$.



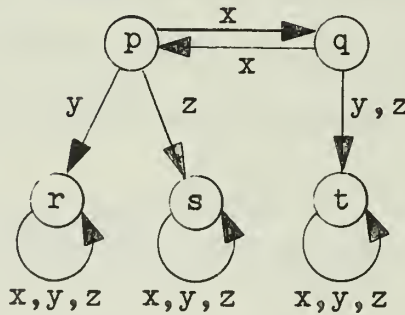
Conditions (i), (ii), and (iii) are clearly satisfied, but there exists no $p \neq q$ in A . Obviously, the only automorphism on A is the identity.

(b) Let $A = (Q, I, \delta)$, with $Q = \{p, q\}$, $M = \{x, y\}$, $\delta(q, x) = \delta(p, x) = p$, and $\delta(q, y) = \delta(p, y) = q$.



Here, there exists $p \neq q$, such that $A(p) = A(q)$. Furthermore, $\delta(q, x) = \delta(p, x)$ and $\delta(q, y) = \delta(p, y) \implies \delta(q, z) = \delta(p, z)$, for all $z \in I \implies$ if $\delta(q, u) = \delta(q, v)$, then $\delta(p, u) = \delta(p, v)$, for any $u, v \in I$. Thus, all conditions of # 5.14 are satisfied, except that $C_x(q)$ is not circular and, indeed, the only automorphism on A is the identity.

(c) Let $A = (Q, I, \delta)$, with $Q = \{p, q, r, s, t\}$, $M = \{x, y, z\}$, $\delta(q, y) = \delta(q, z) = \delta(t, x) = \delta(t, y) = \delta(t, z) = t$, $\delta(p, z) = \delta(s, x) = \delta(s, y) = \delta(s, z) = s$, $\delta(p, x) = q$, $\delta(p, y) = \delta(r, x) = \delta(r, y) = \delta(r, z) = r$, and $\delta(q, x) = p$.



Here, there exists $p \neq q$, such that $A(p) = A(q)$, and $C_x(q)$ is circular. However, condition (iii) is not satisfied and, again, the only automorphism on A is the identity.

Theorem # 5.14 furnishes the basis for determining the existence and nature of the non-trivial automorphisms on an automaton, as will be seen below, when this theorem is applied

to the primaries of the automaton, since an automorphism on A maps each primary onto a primary. Thus, with the aid of theorem # 5.14 and the remarks on extensions of automorphisms in section # 7, below, all automorphisms on A which map each primary onto itself are accounted for and characterized. The remaining automorphisms are those which map at least one primary onto another, and those exist only when two distinct primaries are isomorphic, -- a fact which can be discovered by inspection, if the automata are not too large.

In theorem # 5.14, a non-trivial automorphism $h \in G[A(q)]$ was shown to be characterized by the action of a member x of I on a designated initial state q . In theorem # 5.15, we show that such an automorphism partitions $\text{gen } A(q)$ into disjoint cycles of equal length.

5.15. Theorem: Let $h \in G[A(q)]$ be non-trivial, where $h(q) = \delta(q, x)$. Suppose there exists $r \in \text{gen } A(q) - C_x(q)$. Then,

- (i) $\# [c_h(r)] = \# [C_x(q)]$.
- (ii) $c_h(r) \cap C_x(q) = \emptyset$.

Proof: (i) Let $\# [C_x(q)] = n$ and $\# [c_h(r)] = m$. By ## 5.8 and 5.12, $\# [C_x(q)] = n \implies h^n$ is the identity on $A(q) \implies m \leq n$. But, by # 4.12, h^m is the identity on $A(r) = A(q)$ and, thus, by # 5.8, $n = \# [C_x(q)] \leq m$. Hence, $n = m$.

(ii) By # 5.14, there exists $s \in Q_{A(q)}$ such that $h(r) = s \neq r$, $A(s) = A(r) = A(q)$, $C_y(r)$ is circular, where

$s = \delta(r, y)$, and $\delta(r, z) = \delta(r, t) \implies \delta(s, z) = \delta(s, t)$ for any $z, t \in I$. Now, by # 5.8, $c_h(r) = C_y(r)$, and it remains to show that $C_y(r) \cap C_x(q) = \emptyset$.

Suppose that $p \in C_y(r) \cap C_x(q)$. Then, there exist smallest non-negative integers, i and j , such that $\delta(q, x^i) = p = \delta(r, y^j)$. But then, by # 5.8, $h^i(q) = h^j(r)$. If $j \leq i$, then $r = h^0(r) = h^{i-j}(q) = \delta(q, x^{i-j}) \implies r \in C_x(q)$. If, on the other hand, $i \leq j$, where $\# [c_h(r)] = n$, then $h^{i+n-j}(q) = h^n(r) = r \implies r \in C_x(q)$. Since both alternatives produce a contradiction to the hypothesis, $c_h(r) \cap C_x(q) = \emptyset$.

Q.E.D.

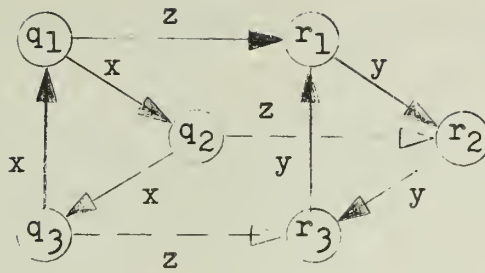
We denote the order of a group element, γ , by $o(\gamma)$.

5.16. Corollary: Let $h \in G[A(q)]$, where $h(q) = \delta(q, x)$. Then, $o(h) = \# [C_x(q)] = \# [c_h(q)]$.

Proof: The corollary follows from ## 4.12 and 5.15.

Q.E.D.

Theorem # 5.17 is merely a collection of technical lemmas, presented here primarily to afford facility of manipulation. Yet, it displays such interrelationships as the following: if $c_h(q_1) = C_x(q_1)$ and $c_h(r_1) = C_y(r_1)$, for $h \in G[A(q)]$ and $q_1, r_1 \in \text{gen } A(q)$, then respective h -successors of q_1 and r_1 are connected in the same manner q_1 and r_1 are connected, as is illustrated in the following partial diagram of an automaton.



5.17. Theorem: Let $A(q) = A(r)$, let $h \in G[A(q)]$, let

$h(q) = p = \delta(q, x)$, and let $h(r) = s = \delta(r, y) = \delta(q, z)$.

Then, for all non-negative integers k ,

$$(i) \delta(q, x^k z) = \delta(q, z y^k);$$

$$(ii) r = \delta(q, u) \iff \delta(r, y^k) = \delta(q, x^k u) \iff$$

$$s = \delta(p, u);$$

$$(iii) q = \delta(r, v) \iff \delta(q, x^k) = \delta(r, y^k v) \iff$$

$$p = \delta(s, v).$$

Proof: (i) $\delta(q, x^k z) = \delta[\delta(q, x^k), z] = \delta[h^k(q), z] = h^k[\delta(q, z)] = h^k(s) = h^k[h(r)] = h[h^k(r)] = h[\delta(r, y^k)] = \delta[h(r), y^k] = \delta[\delta(q, z), y^k] = \delta(q, z y^k)$.

$$(ii) \text{ With } k = 0, \delta(r, y^k) = \delta(q, x^k u) \implies r = \delta(q, u).$$

Now, $r = \delta(q, u) \implies h(r) = h[\delta(q, u)] \implies h(r) = \delta[h(q), u] \implies s = \delta(p, u)$. Furthermore, $s = \delta(p, u) \implies h(r) = h[\delta(q, u)] \implies$ for all $k \geq 0$, $h^k(r) = h^k[\delta(q, u)] \implies \delta(r, y^k) = \delta[h^k(q), u] = \delta[\delta(q, x^k), u] = \delta(q, x^k u)$.

The proof of (iii) is almost identical to that of (ii) and, thus, we omit it.

Q.E.D.

5.18. Theorem: Let $h \in G[A(q)]$, let $h(q) = \delta(q, x)$, and let $p \in Q_{A(q)}$. Then,

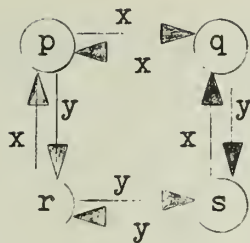
- (i) $o(h) = \# [C_x(q)]$ divides $\# [\text{gen } A(q)]$;
- (ii) $\# [c_h(p)]$ divides $\# [C_x(q)]$.

Proof: (i) By # 5.16, $o(h) = \# [C_x(q)]$ and by # 5.15, for any $r \in \text{gen } A(q)$, $C_x(q)$ and $c_h(r)$ have the same length and are either disjoint or identical. Hence, h partitions $\text{gen } A(q)$ into disjoint cycles, each of length $o(h)$ and, therefore, $o(h)$ divides $\# [\text{gen } A(q)]$.

(ii) Let $o(h) = n$ and $\# [c_h(p)] = m$. Clearly, $m \leq n$ and, hence, $n = sm + t$, for some positive integer s and some non-negative integer $t < m$. Now, $p = h^n(p) = h^{sm+t}(p) = h^t[(h^m)^s(p)] = h^t(p) \implies t = 0$, since $t < m = \# [c_h(p)]$. But then, $n = sm \implies m$ divides n .

Q.E.D.

We note that the existence of a generator, r , of $A(p)$, for which $r = \delta(p, y)$ and such that $\# [C_y(p)]$ does not divide $\# [\text{gen } A(q)]$, does not indicate that $G[A(q)]$ is trivial. It merely shows that, for no $h \in G[A(p)]$ does $h(p) = r$. As an example, let $A = (Q, I, \delta)$, with $Q = \{p, q, r, s\}$, $M = \{x, y\}$, $\delta(p, x) = \delta(s, x) = q$, $\delta(p, y) = \delta(s, y) = r$, $\delta(q, x) = \delta(r, x) = p$, and $\delta(q, y) = \delta(r, y) = s$.



Here, $\# [C_y(p)] = 3$, while $\# [\text{gen } A(p)] = 4$. Yet, $h \in G[A(p)]$, where $h(p) = q$ (and, hence, $h(q) = p$, $h(r) = s$, and $h(s) = r$). Indeed, h is the only non-trivial automorphism on $A(p)$.

5.19. Definition: The set of automorphic images of a state q of an automaton A , denoted by $G(q)$, is defined by,

$$G(q) = \{h(q) : h \in G(A)\}.$$

For any subgroup H of $G(A)$, $H(q) \stackrel{\text{def}}{=} \{h(q) : h \in H\}.$

5.20. Lemma: Let $A = (Q, I, \delta)$ and let $q \in Q$. Then,

- (i) $[G(q), \#]$ is a group, where " $\#$ " is defined by,
 $h(q) \# g(q) = hg(q)$, for any $h, g \in G(A)$;
- (ii) $[G(q), \#]$ is a homomorphic image of $G(A)$;
- (iii) If $A = A(q)$, then $[G(q), \#] \cong G(A)$.

Proof: Let $\theta: G(A) \longrightarrow [G(q), \#]$ be defined by, $\theta(h) = h(q)$, for all $h \in G(A)$. Then, θ is well defined, since each $h \in G(A)$ is well defined on Q . Let $h, g \in G(A)$. Then,
 $\theta(hg) = hg(q) = h(q) \# g(q)$, and θ is a homomorphism. Thus,
 (ii) is proved and, since θ is clearly epic, (i) is proved.

To prove (iii), we note that $q \in \text{gen } A$ and, hence, by # 4.11, distinct members of $G(A)$ have distinct values for q .

Hence, $\# [G(q)] = \# [G(A)]$ and θ is monic. Thus, θ is an isomorphism.

Q.E.D.

5.21. Lemma: Let A be an arbitrary automaton, let H be a subgroup of $G(A)$, and let p and q be any two states of A . Then, either $H(p)$ and $H(q)$ are identical, or they are disjoint.

Proof: Let $t \in H(p) \cap H(q)$. Then, there exist $h, g \in H$, such that $t = h(p) = g(q) \implies g^{-1}h(p) = q$. Now, for any $k \in H$, $k(q) = kg^{-1}h(p) \in H(p) \implies H(q) \subseteq H(p)$. By the symmetry of the argument, we also have $H(p) \subseteq H(q)$ and, hence, $H(p) = H(q)$.

Q.E.D.

5.22. Theorem: $\#(G[A(q)])$ divides $\#[\text{gen } A(q)]$.

Proof: By # 5.21, $G[A(q)]$ partitions $\text{gen } A(q)$ into disjoint subsets of the form $G(p)$ and, by # 5.20, for each such $G(p)$, $\# [G(p)] = \# (G[A(q)])$. Hence, $\#(G[A(q)])$ divides $\#[\text{gen } A(q)]$.

Q.E.D.

We note that # 5.18 (i) follows from # 5.22 as a corollary.

Fleck states as theorem 2 in [5]: If $A = (Q, I, \delta)$ is a strongly connected automaton, then $\# [G(A)] \leq \#(Q)$. Since a

strongly connected automaton is the minimal automaton of each of its states and, since in that case $\text{gen } A = Q$, Fleck's theorem is an immediate corollary to theorem # 5.22. In fact, Fleck's theorem can be strengthened into the following corollary, which follows immediately from theorem # 5.22 and, hence, is stated without proof.

5.23. Corollary: Let $A = (Q, I, \delta)$ be a strongly connected automaton. Then, $\#[G(A)]$ divides $\#(Q)$.

We recall at this point that two members, x and y , of I^* are distinct for $A = (Q, I, \delta)$ if, and only if, there exists $q \in Q$ such that $\delta(q, x) \neq \delta(q, y)$. Thus, since Q is finite, there exists only a finite number of members of I^* distinct for A (even though each may be represented in an infinite number of ways). It is in this sense that we use the term "distinct" in # 5.24 and other results to follow.

5.24. Characterization Theorem: Let $A(q) = (Q, I, \delta)$, and let $\{x_i: 1 \leq i \leq n\}$ be a maximal set of distinct members of I^* satisfying:

(i) $C_{x_i}(q)$ is circular;

(ii) for any $y, z \in I^*$, $\delta(q, y) = \delta(q, z) \implies$

$\delta(q, x_i y) = \delta(q, x_i z)$;

(iii) $\delta(q, x_i) = \delta(q, x_j) \implies i = j \quad (1 \leq i, j \leq n)$.

Then,

(a) any $h \in G[A(q)]$ is defined by $h(q) = \delta(q, x_i)$,

for some $i \in \{1, 2, \dots, n\}$;

- (b) "For all $u \in I^*$, $h_1[\delta(q, u)] = \delta(q, x_1 u)$ " defines an automorphism h_1 on $A(q)$ for each $i \in \{1, 2, \dots, n\}$;
(c) $\#(G[A(q)]) = n$.

Proof: (a) This is immediate from # 5.14.

(b) For each $i \in \{1, 2, \dots, n\}$, since $C_{x_1}(q)$ is circular, there exists a positive integer k , such that $q = \delta(q, x_1^k) = \delta[\delta(q, x_1), x_1^{k-1}]$ and, hence, q is a state of $A[\delta(q, x_1)]$. Thus, $A[\delta(q, x_1)] = A(q)$. Hence, unless $\delta(q, x_1) = \delta(q, \epsilon) = q$ and h_1 is the identity automorphism, (b) follows from # 5.14.

(c) From (a), we have $\#(G[A(q)]) \leq n$ and, from (b), we have $n \leq \#(G[A(q)])$. Hence, $\#(G[A(q)]) = n$.

Q.E.D.

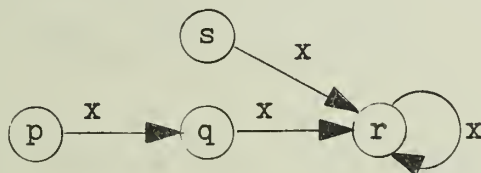
6. PRIMARIES AND AUTOMORPHISMS

6.1. Theorem: Let $f: A = (Q, I, \delta) \longrightarrow A' = (Q', I, \delta')$ be a homomorphism. Then, for each primary P' of $f(A)$, there exists a primary P of A , such that $f(P) = P'$.

Proof: Without loss of generality, let $f(A) = A'$. Let $p' \in Q'$ be such that $P' = A(p')$. Then, there exists $p \in Q$, such that $f(p) = p'$. Now, by # 5.1, $f[A(p)] = A[f(p)] = P'$. By # 2.5, there exists a primary $A(r)$ of A , such that $p \in Q_{A(r)}$ and, hence, there exists $x \in I^*$, such that $\delta(r, x) = p$. Now, $p' = f(p) = f[\delta(r, x)] = \delta'[f(r), x]$ and, hence, $A(p') \ll A[f(r)]$. But then, by # 2.4, $A(p') = A[f(r)] = f[A(r)]$. Since $A(r)$ is a primary of A , the theorem is proved.

Q.E.D.

The reader will note that theorem # 6.1 cannot be strengthened to read, "the homomorphic image of a primary is a primary of the homomorphic image", as may be seen from the following example: Let $A = (Q, I, \delta)$, with $Q = \{p, q, r, s\}$, $M = \{x\}$, $\delta(p, x) = q$, and $\delta(q, x) = \delta(r, x) = \delta(s, x) = r$.



Let f be defined by, $f(p) = p$, $f(q) = f(s) = q$, and $f(r) = r$. Then, f is a homomorphism on A . Now, $P = (\{s, r\}, I, \delta)$ is a

primary of A , yet $f(P) = A(q)$ is not a primary of $f(A) = A(p)$. As might be expected, the stronger statement may be made when f is an isomorphism, as is illustrated by the following theorem.

6.2. Theorem: Let B be a primary of $A = (Q, I, \delta)$ and let $h: A \longrightarrow A' = (Q', I, \delta')$ be an isomorphism. Then, $h(B)$ is a primary of $h(A)$.

Proof: Since B is a primary of A , there exists $q \in Q_B$, such that $B = A(q)$. Then, by # 5.1, $h(B) = A[h(q)]$. Suppose $A[h(q)]$ is not a primary of $h(A)$. Then, there exist $p' \in h(Q) - h(Q_B)$ and $x \in I$, such that $\delta(p', x) = h(q)$. But, since h is an isomorphism, $h(Q) - h(Q_B) = h(Q - Q_B)$ and, hence, there exists $p \in Q - Q_B$ such that $h(p) = p'$. Now, $h(q) = \delta'(p', x) = \delta'[h(p), x] = h[\delta(p, x)]$ and, since h is monic, $q = \delta(p, x)$. But, $p \notin Q_{A(q)}$ and $q = \delta(p, x) \implies A(q) \subsetneq A(p) \implies A(q) = B$ is not a primary of A , contradicting the hypothesis. Hence, $h(B)$ is a primary of $h(A)$.

Q.E.D.

6.3. Corollary: An automorphism of an automaton A maps each primary of A onto a primary of A .

Proof: The corollary is immediate from # 6.2.

Q.E.D.

6.4. Definition: An automorphism $h \in G(A)$ is said to be P-regular if, and only if, $h(B) = B$, for each primary B of A . The set of P-regular automorphisms on A is denoted by $P(A)$.

6.5. Theorem: For any automaton A , $P(A)$ is a normal subgroup of $G(A)$.

Proof: Let $f, g \in P(A)$. Then, for any primary B of A , $f(B) = B = g^{-1}(B) \implies fg^{-1}(B) = f[g^{-1}(B)] = f(B) = B \implies P(A)$ is a subgroup of $G(A)$.

Let $h \in G(A)$, let $k \in P(A)$, and let $A(q)$ be a primary of A . Then, by ## 5.1 and 6.3, $h[A(q)] = A[h(q)]$ is a primary of $A \implies k(A[h(q)]) = A[h(q)] \implies h^{-1}kh[A(q)] = h^{-1}(h[A(q)]) = A(q)$. Hence, $h^{-1}kh \in P(A)$ and, therefore, $P(A)$ is a normal subgroup of $G(A)$.

Q.E.D.

As the following theorem is immediate from ## 5.14 and 6.3, we state it without proof.

6.6. Theorem: Suppose $\#(\text{gen } B) = 1$, for each primary B of an automaton A . Then,

- (i) $P(A)$ is trivial;
- (ii) If $G(A)$ is not trivial, then each non-trivial member of $G(A)$ maps at least one primary of A onto another;
- (iii) If, in addition, no two primaries of A have the same number of states, then $G(A)$ is trivial.

6.7. Theorem: Suppose that, for every pair of primaries, B and C ($B \neq C$), of A , at least one of the following holds:

- (i) $\#(\text{gen } B) \neq \#(\text{gen } C)$;
- (ii) $\#(Q_B) \neq \#(Q_C)$.

Then, $P(A) = G(A)$.

Proof: Let $B = A(q)$ be a primary of A , and let $h \in G(A)$. Then, by # 5.1, $h(B) = A[h(q)]$; i.e., the image of a generator of B is a generator of the image $h(B)$ of B . But, by # 6.3, $h(B)$ is a primary of A and, hence, h maps $\text{gen } A(q)$ onto $\text{gen } h(B)$. Thus, since h is monic, $\#(\text{gen } B) \neq \#(\text{gen } C) \Rightarrow h(B) \neq C$. If, on the other hand, $\#(Q_B) \neq \#(Q_C)$, then $h(B) \neq C$, by # 6.3, since h is monic. Hence, in either case, $h(B) = B$. But, since B was arbitrarily chosen, $G(A) = P(A)$.

Q.E.D.

6.8. Theorem: Let $B_1, B_2, \dots, B_n$ be all the (distinct) primaries of an automaton A , and let $q_i \in \text{gen } B_i$, $1 \leq i \leq n$. Let $h \in P(A)$, and let $h(q_i) = \delta(q_i, x_i)$, $1 \leq i \leq n$. Then,

$$o(h) = \text{l.c.m.}\{\#[C_{x_i}(q_i)]: 1 \leq i \leq n\}.$$

Proof: Let h_i be the restriction of h to B_i , let e_i denote the identity on B_i , let k_i denote the order $o(h_i)$ of h_i in $G(B_i)$, and let $\text{l.c.m.}\{k_i: 1 \leq i \leq n\} = m$. Then, for each $i \in \{1, 2, \dots, n\}$, $h_i^m = e_i$. But then, h^m is the identity on A and, hence, $o(h) \leq m$.

Let p be a positive integer, such that $p < m$. Then, there exists $i \in \{1, 2, \dots, n\}$, such that k_i does not divide p . Hence, there exist non-negative integers, q and r , such that $p = qk_i + r$, where $0 < r < k_i$. Hence, $h_i^p = h_i^r$. But, since $0 < r < k_i$ and $o(h_i) = k_i$, $h_i^r \neq e_i$. Hence, $h_i^p \neq e_i$ and, therefore, $h^p \neq e$ (where e is the identity automorphism

on A). Thus, $o(h) \neq p$, for all positive integers $p < m$. Hence, $o(h) = m$. Now, by # 5.16, $k_1 = \#[C_{x_1}(q_1)]$, for each $i \in \{1, 2, \dots, n\}$, and, by # 5.15, it is immaterial which generator of a primary is selected. The theorem follows.

Q.E.D.

7. EXTENSIONS OF AUTOMORPHISMS

In sections ## 5 and 6, the automorphisms of automata of rank 1 were characterized and counted. Consequently, we have a considerable amount of information about the automorphisms of each primary of an automaton. However, if two primaries have a non-empty intersection, an automorphism of one primary may conflict with an automorphism of the other on the common domain.

In this section, we approach the study of the P-regular automorphisms of an automaton, whose rank is greater than 1, by starting with an automorphism of one primary and studying its extensions to other primaries. First, however, we reduce the problem to its essential scope.

7.1. Definition: Let $\mathbb{P}$ be a subset of the set of primaries of an automaton A . Then, $\bigcup_{P \in \mathbb{P}} P$ is said to be a component of A if, and only if:

(i) for any two primaries, B and C , in $\mathbb{P}$, there exists a sequence $B = P_1, P_2, \dots, P_r = C$ of primaries in $\mathbb{P}$, such that $P_i \cap P_{i+1} \neq A(\emptyset)$, $1 \leq i < r$;

(ii) if D is any primary of A , not in $\mathbb{P}$, then $D \cap P = A(\emptyset)$, for all $P \in \mathbb{P}$

Thus, a component is a minimal separated subautomaton. The following lemma # 7.2 is immediate from the definition # 7.1 and, thus, we state it without proof.

7.2. Lemma: (i) Each primary of an automaton A is contained in a unique component of A .

(ii) Every automaton is uniquely decomposable into components.

(iii) Any two components of an automaton are either disjoint or identical.

(iv) Any union of components of an automaton A is a separated subautomaton of A .

7.3. Theorem: Let $h: A = (Q, I, \delta) \longrightarrow A^\circ$ be an isomorphism, and let C be a component of A . Then, $h(C)$ is a component of $h(A)$.

Proof: By # 6.2, if B is a primary of A , then $h(B)$ is a primary of $h(A)$. Now, let $B_1, B_2 \subseteq Q$, such that $B_1 \cap B_2 \neq \emptyset$. Then, clearly, $h(B_1) \cap h(B_2) \neq \emptyset$. Hence, if $P_1, P_2, \dots, P_r$ is a sequence of non-disjoint primaries of A , then, $h(P_1), h(P_2), \dots, h(P_r)$ is a sequence of non-disjoint primaries of $h(A)$. Thus, the primaries of $h(C)$ satisfy (i) of # 7.1.

Now, let D° be a primary of $h(A)$, such that $D^\circ \cap h(P) \neq A(\emptyset)$, for some primary P in A . Since h is an isomorphism, so is h^{-1} and, hence, $h^{-1}(D^\circ)$ is a primary of A , by # 6.2. Let $h^{-1}(D^\circ) = D$. Then, $h(D) \cap h(P) \neq A(\emptyset) \implies D \cap P \neq A(\emptyset)$, since h is monic. Hence, if P is one of the primaries in C , so is D . Thus, if $C = \bigcup_{i=1}^k P_i$, then $D^\circ = h(P_1)$, for some $i \in \{1, 2, \dots, k\} \implies D^\circ \ll h(C)$. Hence, $h(C)$ is a component of $h(A)$.

Q.E.D.

7.4. Corollary: Let $h \in G(A)$. Then, h maps each component of A onto a component of A .

Proof: The corollary is immediate from ## 7.2 and 7.3.

Q.E.D.

In contrast to # 7.3, the homomorphic image of a component need not be a component of the homomorphic image, as can be seen from the example in remark # 4.15.

7.5. Definition: An automorphism $h \in G(A)$ is said to be C-regular if, and only if, $h(C) = C$ for each component C of A . The set of all C-regular automorphisms on A is denoted by $C(A)$.

7.6. Theorem: For any automaton A , $P(A)$ is a normal subgroup of $C(A)$ and $C(A)$ is a normal subgroup of $G(A)$.

Proof: Let $f, g \in C(A)$. Then, for any component C of A , $f(C) = C = g^{-1}(C)$, by # 7.4. Hence, $fg^{-1}(C) = f[g^{-1}(C)] = f(C) = C$, and thus, $fg^{-1} \in C(A)$. Hence, $C(A)$ is a subgroup of $G(A)$.

Let $h \in G(A)$, let $k \in C(A)$, and let C be a component of A . Then, by # 7.4, $h(C)$ is a component of $A \Rightarrow k[h(C)] = h(C) \Rightarrow h^{-1}kh(C) = h^{-1}[h(C)] = C$. Hence, $h^{-1}kh \in C(A)$ and, therefore, $C(A)$ is a normal subgroup of $G(A)$.

Now, if $h \in P(A)$, then $h(P) = P$, for all primaries P of $A \Rightarrow h(C) = C$, for all components C of $A \Rightarrow h \in C(A) \Rightarrow$

$P(A) \subseteq C(A)$. But then, by # 6.5, $P(A)$ is a normal subgroup of $C(A)$.

Q.E.D.

For ease of reference, we gather some obvious, but useful, facts in a single theorem.

7.7. Theorem: Let n be the number of distinct components of an automaton A , and let $r(C)$ denote the number of distinct primaries of a component C of A . Then,

(i) If $n = 1$, then $G(A) = C(A)$.

(ii) If $r(C) = 1$ for all components C of A , then $P(A) = C(A)$.

(iii) If $C(A)$ is trivial, then any non-trivial automorphism of A maps at least one component of A onto another.

(iv) If $r(C) \neq r(D)$, for every pair, C and D , of components of A , then $G(A) = C(A)$.

The proofs of these results are all immediate.

7.8. Definition: Let U and V be subautomata of A . An automorphism $h \in G(U)$ is said to be extendable to V if, and only if, there exists an automorphism $h' \in G(V)$, which is identical to h on the common domain $U \cap V$.

The extension of h to V by h' is the function $h \vee h': U \cup V \longrightarrow U \cup V$, defined by,

$$(h \vee h')(q) = \begin{cases} h(q), & \text{if } q \in Q_U, \\ h'(q), & \text{if } q \in Q_V. \end{cases}$$

We say that $h \vee h'$ is an extension of h (alt., h') to V (alt., U).

It is immediate from the definition # 7.8 that, $h \vee h' \in G(U \cup V)$ and that, if U and V are primaries of A , then $h \vee h' \in P(U \cup V)$. We shall make implicit use of this fact.

7.9. Lemma: Let U, V , and W be subautomata of A . Let $h \in G(U)$, let $h \vee k$ be the extension of h to V by $k \in G(V)$, and let $(h \vee k) \vee j$ be the extension of $h \vee k$ to W by $j \in G(W)$. Then,

(i) $h \vee (k \vee j)$ is defined and is the extension of h to $V \cup W$ by $k \vee j$;

(ii) $[(h \vee k) \vee j](q) = [h \vee (k \vee j)](q)$, for all $q \in Q_{U \cup V \cup W}$.

Proof: (i) Let $q \in Q_V \cap W$. Then, $q \in Q_{(U \cup V) \cap W}$ and, hence, $j(q) = (h \vee k)(q)$. But, $q \in Q_V \implies (h \vee k)(q) = k(q) \implies j(q) = k(q)$. Hence, $k \vee j$ is defined and is the extension of k to W by j .

Now, let $p \in Q_U \cap (V \cup W)$. If $p \in Q_U \cap V$, then $h(p) = k(p)$ by hypothesis. But, since $k \vee j$ is an extension of k and $p \in Q_V$, $k(p) = (k \vee j)(p)$. Hence, $h(p) = (k \vee j)(p)$. If, on the other hand, $p \notin Q_U \cap V$, then $p \in Q_U \cap W$ and $(h \vee k)(p) = h(p)$, since $p \in Q_U - Q_V$. Moreover, since $p \in Q_{(U \cup V) \cap W}$, and since j is an extension of $h \vee k$, $(h \vee k)(p) = j(p)$ and, hence, $h(p) = j(p)$. But, $p \in Q_W - V \implies j(p) =$

$(k \vee j)(p) \Rightarrow h(p) = (k \vee j)(p)$. Hence, h and $k \vee j$ are identical on their common domain. Since $k \vee j \in G(V \cup W)$, $h \vee (k \vee j)$ is the extension of h to $V \cup W$ by $k \vee j$.

(ii) If $q \in Q_U$, then $(h \vee k)(q) = h(q) \Rightarrow [(h \vee k) \vee j](q) = (h \vee k)(q) = h(q)$, by definition # 7.8. Also by # 7.8, $[h \vee (k \vee j)](q) = h(q)$. If $q \in Q_V$, then $(h \vee k)(q) = k(q) \Rightarrow [(h \vee k) \vee j](q) = k(q)$, by definition # 7.8. Also by # 7.8, $(k \vee j)(q) = k(q) \Rightarrow [h \vee (k \vee j)](q) = k(q)$. If $q \in Q_W$, then $[(h \vee k) \vee j](q) = j(q)$, by definition # 7.8. Also by # 7.8, $(k \vee j)(q) = j(q) \Rightarrow [h \vee (k \vee j)](q) = (k \vee j)(q) = j(q)$. Thus, for all $q \in Q_U \cup V \cup W$, $[(h \vee k) \vee j](q) = [h \vee (k \vee j)](q)$.

Q.E.D.

7.10. Theorem: If U is a primary of an automaton A and $h \in G(U)$, then h is extendable to A if, and only if, h is extendable to the component of A which contains U .

Proof: Let C be the component of A which contains U , and suppose h is extendable to C . Let $h \vee h'$ be the extension of h to C by h' . By ## 7.1 and 7.2, $A - C \ll A$ (where $A - C$ is the automaton $A(Q - Q_C)$), since both C and $A - C$ are separated. Let e denote the identity automorphism on $A - C$ and define $k \stackrel{\text{def}}{=} (h \vee h') \vee e$. Clearly, $k \in G(A)$ and, since $A - C$ is separated, k is the extension of $h \vee h'$ to A (we allow ourselves this liberty with the language of definition # 7.8, as no ambiguity arises) by e , by # 7.3. But

then, by # 7.9, $(h \vee h^0) \vee e = h \vee (h^0 \vee e)$ is the extension of h to A by $h^0 \vee e$. Hence, h is extendable to A .

Conversely, suppose that h is extendable to A . Let $h \vee j$ be the extension of h to A by j and let j^0 be the restriction of j to C . Then, clearly, $h \vee j^0$ is the extension of h to C by j^0 and, hence, h is extendable to C .

Q.E.D.

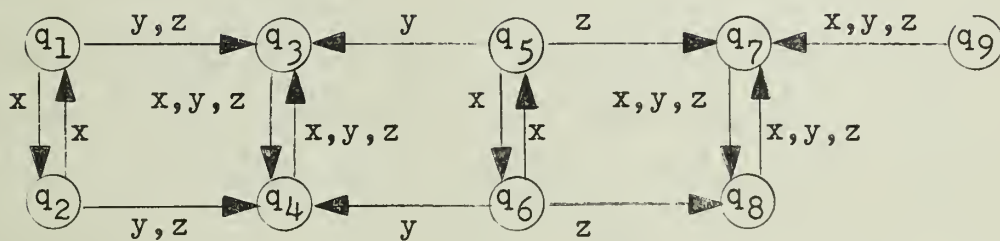
In view of theorem # 7.10, in studying extensions of automorphisms of primaries, we need concern ourselves only with one-component automata; i.e., connected automata. In the remainder of this section, we assume each automaton to be connected. The study of non-C-regular automorphisms is comparable to that of isomorphisms between automata, on which considerable work has been done (see, for example, [3]), and which is outside the scope of this work.

7.11. Theorem: Let U be a primary of an automaton A , and let $h \in G(U)$. If h is extendable to A , then h is extendable to $A[s(U)]$. The converse does not hold.

Proof: Clearly, if k is any extension of h to A , the restriction of k to $A[s(U)]$ is an extension of h to $A[s(U)]$.

To show that the converse does not hold, we consider the following counterexample: Let $A = (Q, I, \delta)$, with $Q = \{q_1: 1 \leq i \leq 9\}$, $M = \{x, y, z\}$, $\delta(q_1, x) = q_2$, $\delta(q_2, x) = q_1$,

$\delta(q_3, x) = \delta(q_3, y) = \delta(q_3, z) = \delta(q_2, y) = \delta(q_2, z) = \delta(q_6, y) = q_4$, $\delta(q_4, x) = \delta(q_4, y) = \delta(q_4, z) = \delta(q_1, y) = \delta(q_1, z) = \delta(q_5, y) = q_3$, $\delta(q_5, z) = \delta(q_8, x) = \delta(q_8, y) = \delta(q_8, z) = \delta(q_9, x) = \delta(q_9, y) = \delta(q_9, z) = q_7$, $\delta(q_5, x) = q_6$, $\delta(q_6, x) = q_5$, and $\delta(q_6, z) = \delta(q_7, x) = \delta(q_7, y) = \delta(q_7, z) = q_8$.



The primaries of A are: B with $Q_B = \{q_1, q_2, q_3, q_4\}$, C with $Q_C = \{q_3, q_4, q_5, q_6, q_7, q_8\}$, and D with $Q_D = \{q_7, q_8, q_9\}$. Define h on B by, $h(q_1) = q_2$, $h(q_2) = q_1$, $h(q_3) = q_4$, and $h(q_4) = q_3$. Then, $h \in G(B)$. As is proved below, in # 7.17, the only extension of h to $A[s(B)] = B \cup C$ is $h \vee h^\circ$, where $h^\circ(q_3) = q_4$, $h^\circ(q_4) = q_3$, $h^\circ(q_5) = q_6$, $h^\circ(q_6) = q_5$, $h^\circ(q_7) = q_8$, and $h^\circ(q_8) = q_7$. Thus, h is extendable to $A[s(B)]$ and it has a unique extension there.

Now, since $\#[\text{gen } D] = 1$, $\#[G(D)] = 1$ by # 5.22 and, hence, the only automorphism on D is the identity. But then, since $(h \vee h^\circ)(q_7) = q_8 \neq q_7$, h is not extendable to A , by # 4.12.

Q.E.D.

We have stated the first part of theorem # 7.11, in spite of the fact that it is immediate from previous results,

since it points the way to establishing the extendability of an automorphism of a primary to the entire automaton, A , and to obtaining all the P -regular automorphisms of A : We start with an arbitrary primary, B , of A and list all non-trivial members of $G(B)$ (These were characterized in §§ 5.14 and 5.24. The author has constructed algorithms, not included in this paper, for finding (i) the primaries of an automaton, (ii) the set of generators of a primary, and (iii) the non-trivial automorphisms of a minimal automaton and, hence, of a primary, the basis for the latter being theorems §§ 5.14 and 5.24. These algorithms are suitable both for hand computation and for computer application and are based on the transition table of the automaton). We find the primaries, B_{11} , B_{21} , ..., $B_{r_1 1}$, other than B , which intersect $s(B)$ (i.e., the primaries, other than B , in $A[s(B)]$) and use our results (primarily # 7.17), below, to find and list all extensions of each automorphism in the list of $G(B)$ to B_{11} . In the same manner, we list all extensions of the automorphisms in the list of $P(B \cup B_{11})$ to B_{21} , and then to B_{31} , ..., $B_{r_1 1}$. The end result is a list of all members of $P(A[s(B)])$.

We now repeat the process; i.e., we find the primaries, B_{12} , B_{22} , ..., $B_{r_2 2}$, in $A[s(A[s(B)])]$ and not in $A[s(B)]$, and list the step-wise extensions in the above manner. The process ends when A is exhausted, or when a list of extensions is empty. In either case, the list includes precisely the non-trivial automorphisms in $P(A)$, where $P(A)$ is trivial in the latter case. That A must be exhausted if $P(A)$ is not trivial, follows from the fact that A has one component; i.e., is connected.

It remains, then, to establish necessary and sufficient conditions for the existence of an extension of an automorphism of a primary to another primary and to count all such extensions. We devote the remainder of this section to this task.

The similarity of conditions in the following results to some of those previously encountered should not surprise the reader, as an extension of an automorphism is still an automorphism in itself. The added requirement we have to satisfy here is that of finding an automorphism which agrees with a given automorphism on their common domain; i.e., which maps specified states in the primary to predetermined states in the same primary. In fact, we first deal with even more simplified version of the problem, -- finding an automorphism which maps one specified state in the primary to another (possibly the same) specified state in the primary. We then study extensions of given automorphisms and, lastly, all P-regular automorphisms on the union of two primaries.

7.12. Lemma: Let $a, b \in Q_{A(q)}$. If $h \in G[A(q)]$ is such that $h(a) = b$, then for each $p \in \text{gen } A(q)$, there exists $r \in \text{gen } A(q)$, such that:

- (i) $C_x(p)$ is circular, where $r = \delta(p, x)$;
- (ii) there exists $y \in I^*$, such that $a = \delta(p, y)$ and $b = \delta(r, y)$;
- (iii) for any $z, w \in I^*$, $\delta(p, z) = \delta(p, w) \implies \delta(r, z) = \delta(r, w)$.

Proof: Let $p \in \text{gen } A(q)$. Then, there exists $y \in I^*$, such that $a = \delta(p, y)$. Let $h(p) = r$. Then, by # 5.1, $r \in \text{gen } A(q)$; i.e., the homomorphic image of a generator is a generator of the homomorphic image. Now, $b = h(a) = h[\delta(p, y)] = \delta[h(p), y] = \delta(r, y)$, and condition (ii) is satisfied..

If $p = r$, conditions (i) (with $x = e$) and (iii) are trivially satisfied, and if $p \neq r$, conditions (i) and (iii) follow from # 5.14 (the existence of some $x \in I^*$ such that $\delta(p, x) = r$ is assured by the fact that $p \in \text{gen } A(q)$). Moreover, condition (iii) makes the choice of x immaterial).

Q.E.D.

7.13. Lemma: Let $a, b \in Q_{A(q)}$ and let $p, r \in \text{gen } A(q)$ be such that (i), (ii), and (iii) of lemma # 7.12 are satisfied. Then,

$h[\delta(p, u)] = \delta(r, u)$, for all $u \in I^*$, defines an automorphism h of $A(q)$, such that $h(a) = b$.

Proof: If $p = r$, then h is the identity on $A(q)$, by # 4.12, and if $p \neq r$, then $h \in G[A(q)]$, by the proof of # 5.14 or by # 5.24 (b); for, if r satisfies conditions (i) and (iii) of our lemma for p , then x satisfies conditions (i) and (ii) of theorem # 5.24, since $r = \delta(p, x)$. Now, by (ii) of our lemma, $a = \delta(p, y) \implies h(a) = h[\delta(p, y)] = \delta(r, y) = b$.

Q.E.D.

7.14. Theorem: Let U and V be primaries of A , and let $h \in G(U)$. Then, h is extendable to V if, and only if,

for some $p \in \text{gen } V$, there exists $r \in \text{gen } V$, such that:

(i) $C_X(p)$ is circular, where $r = \delta(p, x)$;

(ii) for each $a \in Q_U \cap V$, and for each $y \in I^*$ such that $a = \delta(p, y)$, $h(a) = \delta(r, y)$;

(iii) for any $z, w \in I^*$, $\delta(p, z) = \delta(p, w) \implies \delta(r, z) = \delta(r, w)$.

Proof: Suppose that, for some $p \in \text{gen } V$, there exists $r \in \text{gen } V$, such that (i), (ii), and (iii) hold. Then, by # 7.13,

$h'[\delta(p, u)] = \delta(r, u)$, for all $u \in I^*$,

defines an automorphism h' of V , such that $h'(a) = h(a)$, for each $a \in Q_U \cap V$. Hence, h is extendable to V .

Conversely, let $h \vee h'$ be an extension of h to V by $h' \in G(V)$. Then, for each $a \in Q_U \cap V$, $h'(a) = h(a)$ and, hence, by # 7.12, for each $p \in \text{gen } V$, there exists $r \in \text{gen } V$, such that (i), (ii), and (iii) are satisfied.

Q.E.D.

7.15. Theorem: Let $A(q) = (Q, I, \delta)$, let $\delta(q, w) = r$, and let $\{x_i: 1 \leq i \leq n\}$ be a maximal set of members of I^* , distinct for $A(q)$ and satisfying:

(i) $C_{x_1}(q)$ is circular;

(ii) for any $y, z \in I^*$, $\delta(q, y) = \delta(q, z) \implies$

$\delta(q, x_1 y) = \delta(q, x_1 z)$;

(iii) $\delta(q, x_1) = \delta(q, x_j) \implies i = j$ ($1 \leq i, j \leq n$);

(iv) if $\delta(q, x_1 w) = s$ for some $i \in \{1, 2, \dots, n\}$,

then $\delta(q, x_j w) = s$ for all $j \in \{1, 2, \dots, n\}$.

Then,

(a) any $h \in G[A(q)]$ satisfying $h(r) = s$ is defined by $h(q) = \delta(q, x_1)$, for some $i \in \{1, 2, \dots, n\}$;

(b) for each $i \in \{1, 2, \dots, n\}$, "for all $u \in I^*$, $h_i[\delta(q, u)] = \delta(q, x_i u)$ " defines an automorphism h_i on $A(q)$ such that $h_i(r) = s$.

(c) there exist exactly n distinct automorphisms h on $A(q)$ satisfying $h(r) = s$.

Proof: Let $h \in G[A(q)]$ be such that $h(r) = s$. By # 5.24, h is defined by $h(q) = \delta(q, x)$, where $x \in X$ and X is a maximal set of members of I^* distinct for $A(q)$ and satisfying conditions (i), (ii), and (iii). Since $h(r) = s$, we have $s = h(r) = h[\delta(q, w)] = \delta[h(q), w] = \delta(q, xw)$ and, hence, x satisfies all conditions required of the x_i 's. But then, by maximality, for some $i \in \{1, 2, \dots, n\}$, $\delta(q, x) = \delta(q, x_i)$ and, hence, (a) is proved.

From # 5.24 and the fact that each x_i satisfies conditions (i) and (ii), it follows that $h_i \in G[A(q)]$ for each $i \in \{1, 2, \dots, n\}$. Since each x_i satisfies condition (iv), $s = \delta(q, x_i w) = \delta[h_i(q), w] = h_i[\delta(q, w)] = h_i(r)$. Thus, (b) is proved.

Since the x_i 's satisfy condition (iii), (c) follows from (a) and (b).

Q.E.D.

7.16. Lemma: Let $A(p)$ and $A(q)$ be primaries of A , let $h \in G[A(p)]$, and let $h(p) = \delta(p, y)$, for some $y \in I^*$. A necessary and sufficient condition for the existence of an extension of h to $A(q)$ is the existence of $x \in I^*$ which satisfies:

(i) $C_x(q)$ is circular;

(ii) for any $z, w \in I^*$, $\delta(q, z) = \delta(q, w) \implies$

$\delta(q, xz) = \delta(q, xw)$;

(iii) for each $r \in Q_{A(p)} \cap A(q)$ and for any $u, v \in I^*$,

$\delta(p, u) = r = \delta(q, v) \implies \delta(p, yu) = \delta(q, xv)$.

Proof: Let $x \in I^*$ satisfy (i) and (ii). Then, by # 5.24, $k(q) = \delta(q, x)$ defines an automorphism on $A(q)$.

Let $r \in Q_{A(p)} \cap A(q)$ and let $\delta(p, u) = r = \delta(q, v)$. Then, $h(r) = h[\delta(p, u)] = \delta[h(p), u] = \delta(p, yu)$ and, similarly, $k(r) = k[\delta(q, v)] = \delta[k(q), v] = \delta(q, xv)$. Now, if x satisfies condition (iii) as well, then $\delta(p, yu) = \delta(q, xv)$ and, hence, $h(r) = k(r)$. Thus, $h \vee k$ is the extension of h to $A(q)$ by k .

Conversely, suppose there exists an extension, $h \vee j$, of h to $A(q)$ by $j \in G[A(q)]$, and let $r = \delta(p, u) = \delta(q, v)$. Then, by # 7.15, there exists $x \in I^*$ which satisfies (i) and (ii) and, in addition, $j(r) = \delta(q, xv)$. But $h(r) = \delta(p, yu)$ and $h(r) = j(r) \implies \delta(p, yu) = \delta(q, xv)$ and, thus, (iii) is satisfied.

Q.E.D.

7.17. Characterization Theorem: Let $A(p)$ and $A(q)$ be primaries of an automaton A , let $h \in G[A(p)]$ and let $\{x_i: 1 \leq i \leq n\}$ be a maximal set of members of I^* distinct for A and satisfying:

- (i) $C_{x_i}(q)$ is circular;
- (ii) for any $z, w \in I^*$, $\delta(q, z) = \delta(q, w) \implies \delta(q, x_i z) = \delta(q, x_i w)$;
- (iii) $\delta(q, x_i) = \delta(q, x_j) \implies i = j$ ($1 \leq i, j \leq n$);
- (iv) for each $r \in Q_{A(p)} \cap A(q)$, where $r = \delta(q, w)$ for some $w \in I^*$, $h(r) = \delta(q, x_i w)$.

Then,

- (a) any extension of h to $A(q)$ is of the form $h \vee k_1$, where k_1 is defined by, $k_1(q) = \delta(q, x_i)$ for some $i \in \{1, 2, \dots, n\}$;
- (b) for each $i \in \{1, 2, \dots, n\}$, $h \vee k_1$ defines an extension of h to $A(q)$, where k_1 is defined on $A(q)$ by, $k_1[\delta(q, u)] = \delta(q, x_i u)$ for all $u \in I^*$;
- (c) there exist exactly n distinct extensions of h to $A(q)$.

Proof: (a) and (b) follow from # 7.16 and condition (iv). Part (c) follows from (a) and (b) and condition (iii).

Q.E.D.

As a result of theorem # 7.17, we are able to arrive at a characterization and count of all members of $P(B \cup C)$, where B and C are primaries of a given automaton, as is done in the following corollary # 7.18.

7.18. Corollary: Let $A(p)$ and $A(q)$ be primaries of an automaton A . Let $\{t_1, t_2, \dots, t_n\}$ be a maximal set of members of I^* distinct for A and satisfying:

(i) $C_{t_1}(p)$ is circular;

(ii) for any $z, w \in I^*$, $\delta(p, z) = \delta(p, w) \implies$

$\delta(p, t_1 z) = \delta(p, t_1 w)$;

(iii) $\delta(p, t_i) = \delta(p, t_j) \implies i = j \quad (1 \leq i, j \leq n)$.

For each $i \in \{1, 2, \dots, n\}$, let $\{x_{i1}, x_{i2}, \dots, x_{i r_i}\}$ be a maximal set of members of I^* distinct for A and satisfying:

(iv) $C_{x_{i k}}(q)$ is circular;

(v) for any $z, w \in I^*$, $\delta(q, z) = \delta(q, w) \implies$

$\delta(q, x_{i k} z) = \delta(q, x_{i k} w)$;

(vi) $\delta(q, x_{i k}) = \delta(q, x_{i j}) \implies k = j \quad (1 \leq k, j \leq r_i)$;

(vii) for each $r \in Q_{A(p)} \cap A(q)$, $\delta(p, t_i y) = \delta(q, x_{i k} u)$,

where $r = \delta(p, y) = \delta(q, u)$ for some $y, u \in I^*$.

Then,

(a) any $f \in P[A(p) \cup A(q)]$ is of the form $h_i \vee g_{i k}$,

where h_i is defined by $h_i(p) = \delta(p, t_i)$, $1 \leq i \leq n$, on $A(p)$

and, for each such i , $g_{i k}$ is defined on $A(q)$ by $g_{i k}(q) =$

$\delta(q, x_{i k})$, $1 \leq k \leq r_i$.

(b) For each $i \in \{1, 2, \dots, n\}$ and for each $k \in$

$\{1, 2, \dots, r_i\}$, $f = h_i \vee g_{i k}$ defines an automorphism $f \in$

$P[A(p) \cup A(q)]$, where $h_i[\delta(p, u)] = \delta(p, t_i u)$ for all $u \in I^*$,

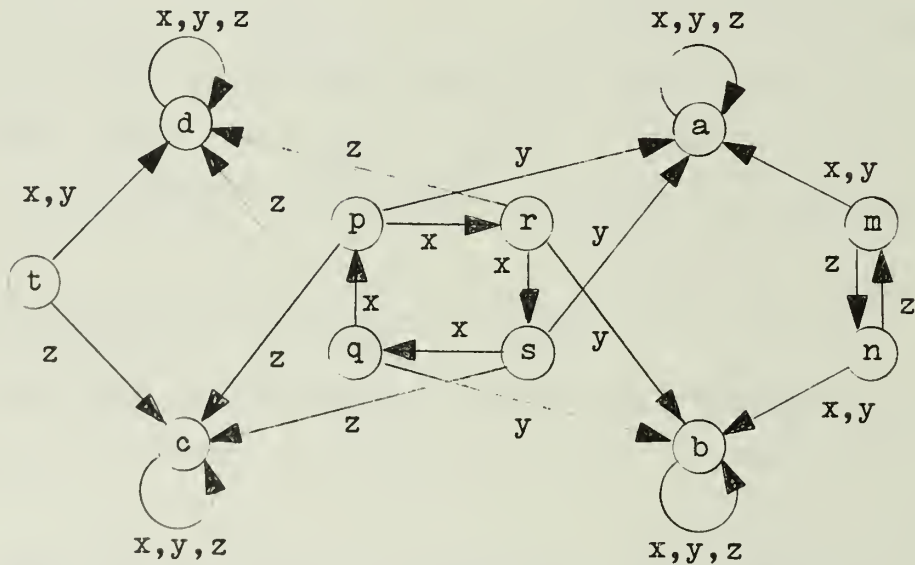
and $g_{i k}[\delta(q, v)] = \delta(q, x_{i k} v)$ for all $v \in I^*$.

(c) $\#(P[A(p) \cup A(q)]) = \sum_{i=1}^n r_i$.

Proof: The corollary is merely a consolidation of the two characterization theorems ## 5.24 and 7.17 (and the results preceding the latter), and it follows with no difficulty from these theorems. Hence, we spare the reader the repetitive nature of the detailed proof.

Q.E.D.

We close this section with a simple example, in which the reader will find an illustration to the results from # 7.12 through # 7.18. Let A be the automaton having the following state diagram:



We recognize in A three primaries: B with states p, q, r, s, a, b, c, d ; C with states t, c, d ; and D with states m, n, a, b . $G(B) = \{h, h^2, h^3, h^4 = e_B\}$, where $h(p) \stackrel{\text{def}}{=} r$. We note that h and h^3 map a to b , b to a , c to d , and d to c , while h^2 maps each of a, b, c, d to itself, as does the identity $h^4 = e_B$ of B . $G(D) = \{k, k^2 = e_D\}$, where $k(m) \stackrel{\text{def}}{=} n$. Since k maps a to b and b to a , both h and h^3 are

extendable to D by k . Similarly, h^2 is extendable to D by $k^2 = e_D$. On the other hand, $G(C) = \{e_C\}$, where e_C is the identity on C . Hence, there exists no extension of either h or h^3 to C , while h^2 is extendable to C by e_C . Thus,

$$P(B \cup D) = \{h \vee k, h^3 \vee k, h^2 \vee e_D, e_B \vee e_D\},$$
$$P(B \cup C) = \{h^2 \vee e_C, e_B \vee e_C\}, \text{ and}$$
$$P(B \cup C \cup D) = \{h^2 \vee e_C \vee e_D, e_B \vee e_C \vee e_D\}.$$

8. ADDITIONAL RESULTS AND POSTSCRIPT

In this section, few lines of further investigation are suggested. The author has achieved some results in one such line, -- quotient automata, and several of these results are reported first.

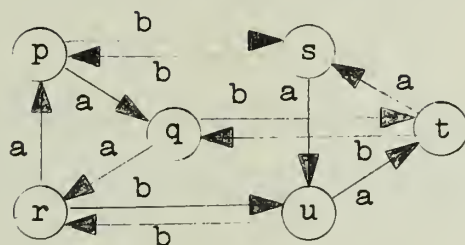
The common definition of an isomorphism between automata requires the latter to have the same input semigroup. Thus, the states of the domain automaton are relabeled by the isomorphism, but the inputs are not. Yet, two automata may be essentially identical, but for the "names" of their states and inputs. We call two such automata essentially isomorphic, abbreviated by "e-isomorphic" (for a precise definition, see Bavel and Muller [10], where a "generalized homomorphism" is defined).

8.1. Representation Theorem: Let $H = (X, \cdot)$ be a finite group of order n . Then, there exists an n -state automaton A_H of rank 1, such that $G(A_H) \cong H \cong I$, where I is the input semigroup of A_H . Moreover, A_H is unique up to e-isomorphism and is strongly connected.

We call A_H of # 8.1 the automaton-representation of the group H . We note that A_H is a reversible automaton (see [10]), since its input semigroup is a group.

By way of an example, consider the dihedral group D_3 of order 6, defined by, $a^3 = b^2 = 1$, $bab = a^{-1}$. A simple compu-

tation shows A_{D_3} to be (essentially uniquely) the following automaton:



8.2. Definition: Let A be an automaton. Then, the automaton induced by A (or, the induced automaton of A) is $A_G(A)$; i.e., the automaton-representation of the group of automorphisms of A .

As an illustration, if A is the automaton described just before # 8.8, below, then its induced automaton is A_{D_3} described just before # 8.2, above.

8.3. Definition:⁽¹⁰⁾ Let $A = (Q, I, \delta)$. A triple $A' = (Q', I', \delta')$ is said to be a semiautomaton of A if, and only if, A' is an automaton, where $Q' \subseteq Q$, I' is a subsemi-group of I , and δ' is the restriction of δ to $Q' \times I'$.

8.4. Theorem: Let H be a subgroup of $G[A(q)]$. Then, $A(q)$ has exactly $\#[\text{gen } A(q)]/\#(H)$ disjoint semiautomata, whose states are generators of $A(q)$, each e-isomorphic to A_H .

(10)

This definition is due to Barnes ([15]), who uses the term "subautomaton". We reserve the latter term for its customary use (see # 0.7).

8.5. Theorem: Let H be a subgroup of $G(A)$, and define γ on A by: $\gamma(q) = H(q)$, for all $q \in Q$ (see definition # 5.19). Then, γ is a homomorphism.

8.6. Definition: Where γ is the homomorphism of # 8.5, $\gamma(A)$ is the quotient automaton of A by H , denoted A/H .

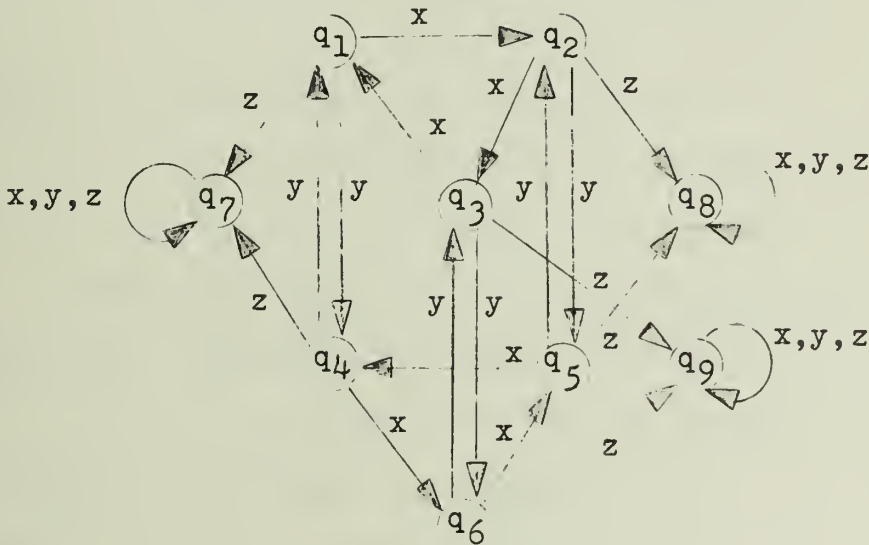
One approach to quotient automata is that of Give'on in [9], where he replaces an entire subautomaton by the trivial automaton (single-state automaton). Definition # 8.6 yields quite a different class of automata. A comprehensive study of quotient automata should probably include a combination of both notions, with definition # 8.6 possibly generalized for less restricted homomorphisms on A .

8.7. Remark: If A is an automaton of rank 1, and H is a subgroup of $G(A)$, then the generators of A/H are precisely the semiautomata of # 8.4. If, in addition, A is strongly connected, then (trivially) the states of A/H are these semiautomata.

Let $\mathbb{A}(H)$ denote the class of all automata A_1 , whose automorphism-group contains, as a subgroup, an isomorphic image H_1 of a given group H . One may study the "essential" differences among members of $\mathbb{A}(H)$ by comparing the quotient automata A_1/H_1 . The following subclasses of $\mathbb{A}(H)$ may yield interesting observations when treated thus: (a) automata of rank 1;

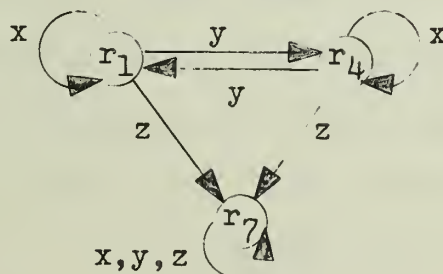
(b) strongly connected automata; (c) automata whose entire group of automorphisms is isomorphic to H ; (d) the intersection of (a) and (c); (e) the intersection of (b) and (c).

A special role is played by the normal subgroups of the automorphism-group of an automaton in connection with quotient automata. We illustrate this role by the following example. Let A be the automaton with the following state-diagram:



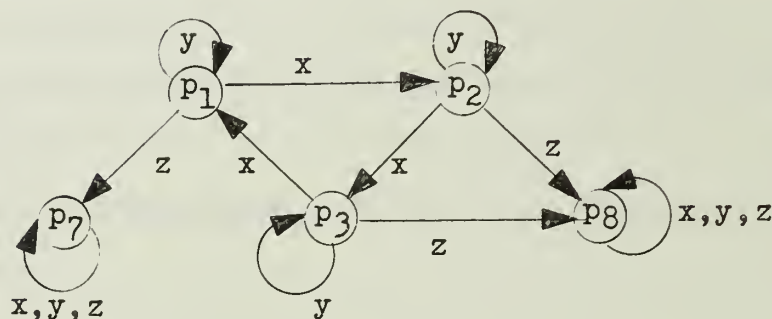
Where $h(q_1) \stackrel{\text{def}}{=} q_2$ and $k(q_1) \stackrel{\text{def}}{=} q_4$, $G(A) = \{e, h, h^2, k, kh, kh^2\} = D_3$.

H is a normal subgroup of $G(A)$, where $H = \{e, h, h^2\}$, and A/H has the following state-diagram:



Here, $G(A/H) = \{e, k'\}$, where $k'(r_1) \stackrel{\text{def}}{=} r_4$. Indeed, $G(A/H) \cong G(A)/H$.

On the other hand, K is not a normal subgroup of $G(A)$, where $K = \{e, k\}$, and A/K has the following state-diagram:



Here, $G(A/K)$ is trivial and not the three-group, as might have been expected.

8.8. Theorem: Let H be a normal subgroup of $G(A)$.

(i) For each $g \in G(A)$, $\gamma_g: A \rightarrow A/H$ is a homomorphism, where $\gamma_g(q) \stackrel{\text{def}}{=} Hg(q)$, for all $q \in Q$.

(ii) For each $g \in G(A)$, g' is an automorphism on A/H , where g' is defined by, $g'(p') = Hg(q) = \{hg(q): h \in H\}$, for each $q \in p' = H(p) \in Q_{A/H}$.

(iii) $G(A)/H$ is isomorphic to a subgroup of $G(A/H)$.

As a consequence of theorem # 8.8 and the remarks preceding it, it appears that an investigation of the normal subgroups of $G(A)$ and their particular role in quotient automata is desirable. Such an investigation proves to be rather extensive and, at this point, we shall just mention two of the normal subgroups of $G(A)$, in addition to $P(A)$ and $C(A)$, already defined (in # 6.4 and # 7.5 respectively).

8.9. Definition: $f \in G(A)$ is s.c.-regular if, and only if, $f(B) = B$, for all strongly connected $B \ll A$. The set of all s.c.-regular functions on A is denoted by $F(A)$.

8.10. Definition: $k \in G(A)$ is completely regular if, and only if, $k(B) = B$, for every $B \ll A$. The set of all completely regular functions on A is denoted by $K(A)$.

We note that $F(A)$ and $K(A)$ are normal subgroups of $G(A)$ and that we may have, $\{e\} \subsetneq K(A) \subsetneq F(A) \subsetneq G(A)$.

The author has partially studied a variety of normal subgroups of $G(A)$, and has obtained several interesting results concerning them. However, considerably more should be looked into before this investigation may be organized; for example, composition series of automata and their correspondence to the generating series of subgroups, Jordan-Holder type of treatment, and the like.

One other interesting avenue of investigation is the generalization of the present work to monadic algebras. As an illustration, the definition of primary may not be useful or, indeed, may not even apply to an algebra, as is the case with the algebra of all integers under addition of 1. To generalize to the algebra $A = (Q, M, \delta)$, we call $R \subseteq Q$ singly generated if, and only if, there exists $r \in Q$, such that $R \subseteq \delta(r)$. We

call $R \subseteq Q$ finitely closed if, and only if, every finite subset of R is singly generated by a member of R . Then, we call (R, M, δ) a primary of A if, and only if, R is a maximal finitely closed subset of Q .

An obvious direction is that of applying such tools as are presented in this paper to sequential machines with output. We expect the source and the primary to be useful, for instance, in investigating experiments, length of experiments (see, for example, Ginsburg [3]) and total length of experiments (see, for example, Bavel [16]). In fact, these two structures are basic enough to be of use in most areas of the theory of automata and sequential machines.

Another interesting area of investigation is the application of the results on automorphisms, presented and hinted at here, to group theory. As a particular example, the automaton-representation of a group may furnish the group theorist with a means of observing his finite group "in action", and draw some additional insights as a result.

Other avenues of mathematical investigation suggest themselves, as well as the possibility of finding interesting applications of these results in the various fields employing weighted, directed graphs (Hohn, Seshu, and Aufenkamp [17]), i.e., automata, for the representation of the natural systems under investigation.

BIBLIOGRAPHY

- [1] Rabin, M. O., and Scott, D., "Finite Automata and Their Decision Problems." IBM J. Res. Dev. 3 (April 1959) 114 - 125.
- [2] Ginsburg, S., "Some Remarks on Abstract Machines." Trans. Amer. Math. Soc. 96 (1960), 400 - 444.
- [3] Ginsburg, S., An Introduction to Mathematical Machine Theory. Addison-Wesley Publishing Co., Inc., Reading, Massachusetts (1962).
- [4] Fleck, A. C., "Structure Preserving Properties of Certain Classes of Functions on Automata." Computer Laboratory, Mich. St. U., May 1961 (unpublished paper).
- [5] Fleck, A. C., "Isomorphism Groups of Automata." J. ACM 9,4 (October 1962) 469 - 476.
- [6] Weeg, G. P., "Some Group Theoretic Properties of Strongly Connected Automata." Computer Laboratory, Mich. St. U., May 1961 (unpublished paper).
- [7] Weeg, G. P., "The Structure of an Automaton and Its Operation Preserving Transformation Group." J. ACM 9, 3 (July 1962) 345 - 349.
- [8] Moore, E. F., "Gedanken Experiments on Sequential Machines." In Automata Studies, Princeton U. Press, Princeton, New Jersey (1956) 129 - 153.
- [9] Give'on, Y., "Toward a Homological Algebra of Automata." Dept. of Comm. Sc., U. of Michigan, February 1965 (unpublished paper).
- [10] Bavel, Z., and Muller, D. E., "Reversibility in Monadic Algebras and Automata." Proc. Sixth Annual Symposium, Switching Circuit Theory and Logical Design, 1965 (to be published).
- [11] Huzino, S., "On Some Sequential Machines and Experiments." Mem. Fac. Sci. Kyushu Univ., ser. A, 12 (1958), 136 - 158.
- [12] Huzino, S., "Theory of Finite Automata." Mem. Fac. Sci. Kyushu Univ., ser. A, 15 (1961), 97 - 159.
- [13] Gluschkow, Theorie der Abstrakten Automaten. Veb Deutscher Verlag der Wissenschaften, Berlin (1963).
- [14] Kelly, J. L., General Topology, D. Van Nostrand Co., Inc., Princeton, New Jersey (1955).

- [15] Barnes, B., "Relationships Between Groups of Isomorphisms and Set of Equivalence Classes of Input for Automata."
(Presented to ACM National Conference at Denver, Colorado. August, 1963. Unpublished paper).
- [16] Bavel, Z., "On the Total Length of an Experiment, I." Proc. Fifth Annual Symposium, Switching Circuit Theory and Logical Design, 1964.
- [17] Hohn, F. E., Seshu, S., and Aufenkamp, D. D., "The Theory of Nets." I.R.E. Transactions on Electronic Computers, Vol. EC - 6, September, 1957. # 3, 154 - 161.

ALTA

Zamir Bavel was born in Tel-Aviv, Israel, on February 8, 1929. He graduated from Levinsky Teachers College in Tel-Aviv in 1947, and was a teacher and assistant principal in Tel-Aviv until 1952. In 1952, he entered Southern Illinois University at Carbondale, Illinois, from which institution he received the A.B., B.S., and B.Mus. degrees in 1954 with highest honors. In 1955, he received the M.A. degree from the same institution, and taught there until 1962. He has attended the University of Illinois since then. He is a member of Delta Rho, Kappa Delta Pi, the American Mathematical Society, the Mathematical Association of America, and the Association for Computing Machinery.



UNIVERSITY OF ILLINOIS-URBANA
510.84 IL6R no. C002 no.188-199(1965
Internal report /



3 0112 088398232